? t s3/3

3/3/1 **Links**

Derwent WPI

0012348951 *Drawing available*

WPI Acc no: 2002-291314/200233

Related WPI Acc No: 2004-794218

XRPX Acc No: N2002-227456

Packet communication apparatus e.g. LAN switch, has state managers which receive directive packets to change state of network interfaces for forwarding packets

Patent Assignee: HITACHI LTD (HITA); NOZAKI S (NOZA-I); SAWADA S (SAWA-I); WATANUKI T (WATA-I)

Inventor: NOZAKI S; SAWADA S; TATSUMI Y; WATANUKI T

Patent Family (3 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20020016858	A1	20020207	US 2001893004	A	20010628	200233	B
JP 2002084306	A	20020322	JP 2001195692	A	20010628	200236	E
US 6907470	B2	20050614	US 2001893004	A	20010628	200540	E

Priority Applications (no., kind, date): US 2001893004 A 20010628; JP 2000195706 A 20000629

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
US 20020016858	A1	EN	51	38		
JP 2002084306	A	JA	52			

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-084306

(43)Date of publication of application : 22.03.2002

(51)Int.Cl. H04L 12/46
H04L 12/02
H04L 12/22
H04L 12/44
H04L 12/56

(21)Application number : 2001-195692

(22)Date of filing : 28.06.2001

(71)Applicant : HITACHI LTD

(72)Inventor : SAWADA SUNAO
WATANUKI TATSUYA
NOZAKI SHINJI
TATSUMI YOSHIYUKI

(30)Priority

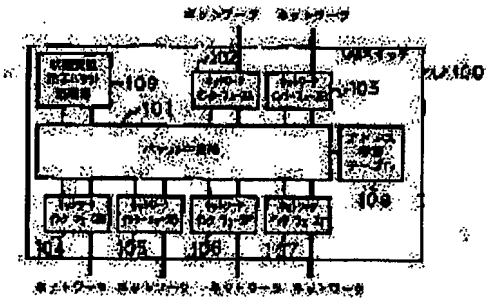
Priority number : 2000195706 Priority date : 29.06.2000 Priority country : JP

(54) PACKET COMMUNICATION APPARATUS AND NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an unauthorized user from using a network system, in an unauthorized manner.

SOLUTION: A LAN 100 is provided with a packet relay part 101, a plurality of network interfaces 102 to 107, an address learning table 108 and a state change instruction packet processing part 109. In the processing part 109, a state change instruction packet which holds an instruction to change the state of a specific network interface to a 'connective state', a 'nonconnective state' or a 'no state' is received from an authentication server 401 via the part 101, and the state change instruction packet is transmitted to a state control part 203 inside the specific network interface. In the part 203, on the basis of the state change instruction packet, the state of the specific network interface is changed into the 'connective state', the 'nonconnective state' or the 'no state'.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－84306
（P2002－84306A）
(43)公開日　平成14年３月22日(2002.3.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04L	12/46		H04L	12/46	M　5K030
		200			200S　5K033
	12/02			12/02	A
	12/22			12/22	
	12/44	300		12/44	300

審査請求　未請求　請求項の数６　ＯＬ　（全 52 頁）　最終頁に続く

(21)出願番号　特願2001－195692(P2001－195692)
(22)出願日　平成13年６月28日(2001.6.28)
(31)優先権主張番号　特願2000－195706(P2000－195706)
(32)優先日　平成12年６月29日(2000.6.29)
(33)優先権主張国　日本（ＪＰ）

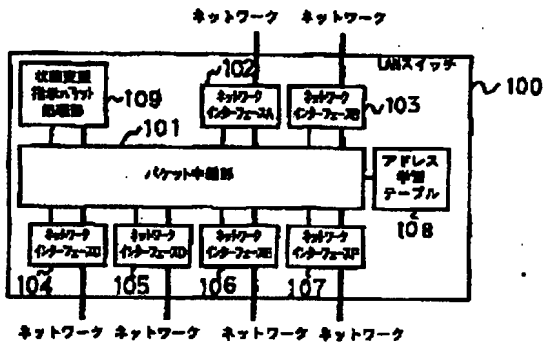
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　澤田　素直
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
(72)発明者　錦貫　達哉
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　パケット通信装置及びネットワークシステム

(57)【要約】
【課題】　不正なユーザがネットワークシステムを不正に利用することを防止する。
【解決手段】　ＬＡＮ１００は、パケット中継部１０１、複数のネットワークインターフェース１０２～１０７、アドレス学習テーブル１０８及び状態変更指示パケット処理部１０９を備え、状態変更指示パケット処理部１０９は、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する指示を保持する状態変更指示パケットを、パケット中継部１０１を介して認証サーバ４０１から受信すると共に、この状態変更指示パケットを、特定のネットワークインターフェース内の状態管理部２０３に送信する。この状態管理部２０３は、状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する。

図１



1

【特許請求の範囲】

【請求項１】ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、

複数のネットワークインターフェースと、

パケットを送信すべき前記ネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、

前記学習テーブルを参照して、前記ネットワークインターフェースの状態に基づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、

特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、前記パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、

特定のネットワークインターフェース内にそれぞれ設けられ、前記状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、該状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部とを備えたパケット通信装置。

【請求項２】前記ネットワークシステムでは、ネットワーク及びルータを介して配されたユーザ端末に動的にアドレスを配布するアドレス割り当てサーバをさらに備え、

受信したパケットの送信元アドレスを登録するフィルタリングテーブルをさらに備え、

前記状態変更指示パケット処理部は、

前記フィルタリングテーブルに登録された特定のアドレスを、前記アドレス学習テーブルに登録するように指示する状態変更指示パケットを受信した場合、該特定のアドレスをアドレス学習テーブルに登録し、

パケットの宛先アドレスが、アドレス学習テーブルに登録されている場合、パケットを中継し、

パケットの宛先アドレスが、アドレス学習テーブルに未登録であり、かつ、前記フィルタリングテーブルに登録され、パケットの送信元アドレスが、ルータ又は認証サーバである場合、パケットを中継するようにした請求項１に記載のパケット通信装置。

【請求項３】前記ネットワークインターフェースは、ネットワークが使用可能であるかどうかを検出する回線断検出部をさらに備え、

前記状態管理部は、

前記回線断検出部により回線断が検出された場合、回線断が検出されたネットワークインターフェースの状態を非接続状態に変更し、

2

前記認証サーバによりユーザ端末が認証を受けた場合、該ユーザ端末に接続されたネットワークインターフェースの状態を接続状態に変更し、

前記パケット中継部は、

非接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態又は接続状態のネットワークインターフェースには中継せず、特定のネットワークインターフェースにのみ中継し、

接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態のネットワークインターフェースには中継しないようにした請求項１又は２に記載のパケット通信装置。

【請求項４】ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、

ネットワークに接続するための物理インターフェースと、

パケットの中継先を選択するパケット中継部と、

パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、前記フィルタリングテーブルの内容に基づいて、パケットを廃棄又は前記パケット中継部に送信するパケット処理部とを有し、前記物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、

前記フィルタリング処理部に対して、前記認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定された前記フィルタリングテーブル内の情報を、前記認証サーバからの指示に基づいて変更し、前記認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットを前記ファイルサーバに中継するための情報を、前記フィルタリングテーブルに順次追加するフィルタリング変更指示処理部とを備えたパケット通信装置。

【請求項５】ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、

ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、

認証サーバにより認証を受けたユーザ端末のアドレスを登録するＩＰアドレス登録表と、

前記ＩＰアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、ＩＰアドレス登録表に未登録のアドレスを送信元アドレスとするパケットはカプセル化した後、特定のアドレス宛に送信するパケット中継部とを備えたパケット通信装置。

【請求項６】請求項１乃至５のいずれかに記載のパケット通信装置と、

前記パケット通信装置にネットワークを介して接続され

たユーザ端末と、
ファイルサーバと、
前記ユーザ端末に対して、前記ファイルサーバへのアクセスを許可するための認証を行う認証サーバとを備えたネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、パケット通信装置及びネットワークシステムに係り、特に、ＬＡＮスイッチやルータ等を用いてネットワークが不正に使用されることを防止する為のパケット通信装置及びネットワークシステムに関する。

【０００２】

【従来の技術】近年、各種ネットワークが保持する情報に対する信用を確保するために、ネットワークの利用を制限する情報セキュリティ技術の必要性が認識されている。一方、ネットワークの利便性を考えて、例えば、ＩＥＥＥ（Institute of Electrical and Electronics Engineers, Inc.）で規定されているＣＳＭＡ／ＣＤ（Carrier Sense Multiple Access with Collision Detection）型の８０２．３ネットワークに代表されるＬＡＮ（Local Area Network）では、ネットワークに端末を接続しさえすれば使用できるようになっている。

【０００３】また、ＩＥＴＦ（Internet Engineering Task Force）で標準化されたＤＨＣＰ（Dynamic Host Configuration Protocol）を用いれば、新たに接続された端末に対して自動的にアドレスが割り当てられ得る。これらのネットワークとノート型パソコンのような可搬型の端末により、端末の利用者が自由な場所で必要な時にネットワークを利用できる情報コンセントシステムが登場している。この情報コンセントシステムに関する技術としては、例えば、特開平１１－６８７６５号公報に記載されたものがある。

【０００４】

【発明が解決しようとする課題】しかしながら、ネットワークの利用が容易になることで、ネットワークの使用許可を得ていない不正な利用者（不正ユーザ）であっても、ネットワークに端末を接続しさえすればネットワークを利用できてしまう場合が想定される。このため、ネットワークに接続されたファイルサーバなどの資源は、不正ユーザからの不正なアクセスにさらされるというセキュリティ上の不都合が生じる。

【０００５】こうした不正ユーザによる不正なアクセスの防止に用いられる技術として、ルータ等のパケット通信装置による“パケットフィルタリング”が知られている。しかし、パケットフィルタリングの条件は予め設定しておかなければならない。それに対して、上述の情報コンセントシステムのように、任意の位置で動的に配布されたアドレスが端末により用いられるネットワークでは、予めパケットフィルタリングの条件を決めておくことは困難である。

【０００６】本発明は、以上の点に鑑み、不正ユーザがネットワークを不正に利用することを防止するパケット通信装置及びネットワークシステムを提供することを目的とする。

【０００７】また、本発明は、ユーザがユーザ端末を自由な位置で、その度に違うアドレスを用いてネットワークに接続しても、そのユーザに対して許可されたネットワーク資源にしかそのユーザがアクセスできないパケット通信装置及びネットワークシステムを提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明によれば、ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、複数のネットワークインターフェースと、パケットを送信すべきネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、学習テーブルを参照して、ネットワークインターフェースの状態に基づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、特定のネットワークインターフェース内にそれぞれ設けられ、状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部とを備えたパケット通信装置が提供される。

【０００９】また、本発明によれば、ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、ネットワークに接続するための物理インターフェースと、パケットの中継先を選択するパケット中継部と、パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、フィルタリングテーブルの内容に基づいて、パケットを廃棄又はパケット中継部に送信するパケット処理部とを有し、物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、フィルタリング処理部に対して、認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定されたフィルタリングテーブル内の情報を、認証サーバからの指示に基づいて変更し、認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットをファイル

5

サーバに中継するための情報を、フィルタリングテーブルに順次追加するフィルタリング変更指示処理部とを備えたパケット通信装置が提供される。

【００１０】また、本発明によれば、ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、認証サーバにより認証を受けたユーザ端末のアドレスを登録するＩＰアドレス登録表と、ＩＰアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、ＩＰアドレス登録表に未登録のアドレスを送信元アドレスとするパケットをカプセル化した後、特定のアドレス宛に送信するパケット中継部とを備えたパケット通信装置が提供される。

【００１１】本発明の特徴のひとつは、パケット通信装置が複数のネットワークインターフェースと、パケット中継部と、各ネットワークインターフェースが接続状態、非接続状態、状態なしのいずれの状態であるかを保持する状態管理部とを有することである。そして、各ネットワークインターフェースの状態がパケット中継部におけるパケットの中継先の選択に影響する。

【００１２】本発明の他の特徴は、パケット通信装置が、状態変更指示パケット処理部を有し、状態変更指示パケットで指示されたネットワークインターフェースの状態を該状態変更指示パケットで指示された状態に変更することができることである。

【００１３】本発明の他の特徴は、各ネットワークインターフェースが回線断検出部を有し、回線断検出部により回線断が検出されると、パケット通信装置はネットワークインターフェースの状態を非接続状態に変更することができることである。

【００１４】本発明においては、初期化時に各ネットワークインターフェースの状態が非接続状態に初期化されるようにしてもよい。

【００１５】本発明の他の特徴は、パケット通信装置が、非接続状態のネットワークインターフェースから受信したパケットを特定のネットワークインターフェースのみに中継することができることである。

【００１６】本発明においては、パケット通信装置が、非接続状態のネットワークインターフェースから受信したパケットを、非接続状態あるいは接続状態のネットワークインターフェースに中継しないようにしてもよい。

【００１７】本発明においては、パケット通信装置が、接続状態のネットワークインターフェースから受信したパケットを非接続状態の該ネットワークインターフェースに中継しないようにしてもよい。

【００１８】本発明においては、認証を行ったユーザの使用する端末が接続されたネットワークインターフェースの状態を、パケット通信装置が接続状態に変更するようにしてもよい。

6

【００１９】本発明の他の特徴は、複数のネットワークインターフェース、パケット中継部、フィルタリングテーブル、フィルタリングテーブルの内容によってパケットフィルタリングを行うパケットフィルタリング部、及びフィルタリングテーブルの内容を外部からの指示により変更するフィルタリング変更指示処理部を有し、初期状態では全ての受信パケットを廃棄するようにフィルタリングテーブルの内容が設定されたパケット通信装置に対して、特定の送信元アドレスを持つパケットの中継を許可する内容を、外部からの指示によってフィルタリングテーブルに順次追加していくことができることである。

【００２０】本発明においては、フィルタリングテーブルに順次追加していく内容は、認証を受けたユーザが使用する端末のアドレスを送信元アドレスとして持つパケットの中継許可を示す情報であってもよい。

【００２１】本発明の他の特徴は、パケット通信装置が複数のネットワークインターフェース、パケット中継部、フィルタリングテーブル、アドレス学習テーブル及び状態変更指示パケット処理部を有し、受信したパケットの送信元アドレスをフィルタリングテーブルに登録し、フィルタリングテーブル内に登録された特定のアドレスをアドレス学習テーブルに登録するよう指示する状態変更指示パケットを受信した場合に、状態変更指示パケット処理部がフィルタリングテーブルに登録された特定のアドレスをアドレス学習テーブルに登録することである。

【００２２】本発明において、パケット通信装置は、学習テーブルに登録されたアドレス宛のパケットを中継し、学習テーブルに登録されてなく、かつ、フィルタリングテーブルに登録されているアドレス宛のパケットについては、特定の送信元アドレスを有している場合にのみ中継することができるようにしてもよい。

【００２３】本発明において、パケット通信装置は、認証を受けたユーザの使用する端末のアドレスを学習テーブルに登録することを指示されることができる。

【００２４】本発明において、パケット通信装置は、複数のネットワークインターフェース、パケット中継部、及びアドレス登録表を有し、アドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットについては、そのパケットをカプセル化した後、特定のアドレス宛に送信するようにしてもよい。

【００２５】本発明において、パケット通信装置が、アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットをカプセル化して送信する際の宛先のアドレスは、ユーザの認証を行う装置のアドレスであ

ってもよい。

【００２６】本発明において、パケット通信装置は、認証を受けたユーザの使用する端末のアドレスをアドレス登録表に登録するようにしてもよい。

【００２７】本発明において、パケット通信装置の各ネットワークインターフェースが「非接続状態」かどうかを管理し、「非接続状態」である場合、通信を遮断するようにしてもよい。

【００２８】本発明において、ネットワークから端末が離脱した場合、この離脱を検出したネットワークインターフェースが、自動的に「非接続状態」に切り替えるようにしてもよい。

【００２９】本発明において、パケット通信装置が、ユーザに対して割り当てられたアドレスを把握し、この把握したアドレスに基づいてパケットフィルタリングの設定を行うようにしてもよい。

【００３０】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を詳細に説明する。

【００３１】図１は、本発明の一実施形態におけるパケット通信装置の構成図である。

【００３２】ＬＡＮスイッチ１００は、例えば、パケット中継部１０１、複数のネットワークインターフェース１０２～１０７、アドレス学習テーブル１０８及び状態変更指示パケット処理部１０９を備える。ネットワークインターフェース１０２～１０７には、それぞれを一意に識別するために名前（図ではＡ～Ｆ）が割り当てられている。なお、名前は、一意に識別できれば番号等であってもよい。

【００３３】これらのネットワークインターフェース１０２～１０７は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。なお、本実施の形態では、ネットワークとしてＩＥＥＥで規定されているＣＳＭＡ／ＣＤ型の８０２．３ネットワークを、ツイストペア線で接続することを想定しているが、本発明は、その他のネットワーク（例えば無線ネットワーク）にも適用可能である。

【００３４】パケット中継部１０１は、全てのネットワークインターフェース１０２～１０７と接続されており、ＯＳＩ（Open System Interconnection）参照モデルのデータリンク層でパケット中継を行う。アドレス学習テーブル１０８には、パケット中継部１０１がパケットを送信すべきネットワークインターフェースを判断するために必要な情報が格納されている。

【００３５】図３は、アドレス学習テーブル１０８の構成図（１）である。

【００３６】アドレス学習テーブル１０８の各エントリは、アドレスフィールド３０１と送信ポートフィールド３０２を含む。アドレスフィールド３０１には、物理アドレス（以下、ＭＡＣアドレスと記す）が、送信ポートフィールド３０２には、ネットワークインターフェースの名前が、それぞれ格納される。ここで、アドレス学習テーブル１０８の各エントリは、パケットを中継する際、パケットの宛先アドレスがアドレスフィールド３０１に一致した場合、同じエントリの送信ポートフィールド３０２で示されるネットワークインターフェースから、パケットを送信することを表している。なお、送信ポートフィールド３０２には、複数のネットワークインターフェースを登録することができる。例えば、特殊なケースとして、ＬＡＮスイッチ１００自体のＭＡＣアドレスをアドレスフィールド３０１に登録し、送信ポートフィールド３０２を「Ｘ」とした場合、このエントリは、該当するパケットを、ＬＡＮスイッチ１００宛のパケットとして処理することを示している。

【００３７】状態変更指示パケット処理部１０９は、ＬＡＮスイッチ１００に接続されたいずれかのネットワークを介して、外部（例えば、後述する認証サーバ４０１）よりＬＡＮスイッチ１００宛に送られた状態変更指示パケットを、パケット中継部１０１を介して受信する。また、状態変更指示パケット処理部１０９は、この状態変更指示パケットの内容を適当なネットワークインターフェース１０２～１０７に通知する。状態変更指示パケットは、特定のネットワークインターフェースの状態を特定の状態に変更する指示を情報として保持している。なお、プロトコルとしては、例えば、ＳＮＭＰ（Simple Network Management Protocol）を使用するが、他にもｔｅｌｎｅｔ（telecommunications network protocol）やＨＴＴＰ（Hyper Text Transfer Protocol）などのプロトコルを利用してもよい。また、本実施の形態では、パケット通信装置としてＬＡＮスイッチ１００を使用しているが、ルータ等その他のパケット通信装置に対しても、本発明は適用可能である。

【００３８】図２は、ネットワークインターフェース１０２～１０７の構成図である。

【００３９】ネットワークインターフェース１０２～１０７は、例えば、ネットワークに接続するための物理インターフェース２０１、ネットワークが使用可能であるかどうかを検出する回線断検出部２０２及びネットワークインターフェースの状態を管理する状態管理部２０３を備え、物理インターフェース２０１と状態管理部２０３は、パケット中継部１０１にそれぞれ接続されている。

【００４０】回線断検出部２０２は、ネットワークの回線（ケーブル）が接続されているかどうか、又は回線を介して接続されている端末が使用可能な状態（電源投入状態）であるかどうかを電気的に検出する。また、回線断検出部２０２は、検出された回線断を状態管理部２０３に通知する。本実施の形態では、回線断検出部２０２が回線断を検出するにあたって、物理インターフェース２０１から通知されるリンクダウン状態が１００ｍｓ以

上続いた場合に、回線断と判定している。なお、回線として光ファイバを用いている場合は光信号の有無が、無線ならば電波の有無がそれぞれ同様に回線断の検出に使用できる。

【００４１】状態管理部２０３は、ネットワークインターフェースの状態が「接続状態」、「非接続状態」及び「状態なし」のいずれであるかを管理する。ユーザ（スイッチ管理者）は、各ネットワークインターフェース１０２～１０７の状態管理部２０３に対して、常に「接続状態」または「状態なし」になるように予め設定することができる。各ネットワークインターフェース１０２～１０７の状態は、ユーザによる設定があればそのように、設定がなければ「非接続状態」となる。また、回線断検出部２０２により回線断が状態管理部２０３に通知されると、ユーザによる事前の設定がない場合、該当するネットワークインターフェースの状態は「非接続状態」になる。さらに、状態変更指示パケット処理部１０９による指示があった場合、その指示に基づいて該当するネットワークインターフェースの状態は上述の三つの状態のいずれかに変更される。

【００４２】つぎに、図４に示されたネットワークシステムを例に、本発明に関するパケット通信装置を用いたネットワークシステムの動作を説明する。

【００４３】図４は、本実施形態におけるＬＡＮ１００を用いたネットワークシステムの構成図である。

【００４４】このネットワークシステムは、例えば、ＬＡＮスイッチ１００（ＭＡＣアドレス２２：２２：００：ＦＦ：ＦＦ：ＦＦ）と、ＬＡＮスイッチ１００のネットワークインターフェースＡ１０２に接続された認証サーバ４０１（ＭＡＣアドレス２２：２２：００：１１：１１：１１）と、ネットワークインターフェースＢ１０３に接続されたファイルサーバ４０２（ＭＡＣアドレス２２：２２：００：２２：２２：２２）と、ネットワークインターフェースＣ１０４～Ｆ１０７にそれぞれ接続され、ユーザが端末を自由に接続してネットワークを利用できる、いわゆる情報コンセント４０９と、情報コンセント４０９を介してネットワークインターフェースＣ１０４に接続されたユーザ端末４０３（ＭＡＣアドレス２２：２２：ＦＦ：００：００：０１）とを備える。

【００４５】認証サーバ４０１は、ユーザがネットワークの使用を許可されているかどうかを判断し、その結果をＬＡＮスイッチ１００に通知する。本実施の形態では、ユーザの認証を、ユーザＩＤとパスワードを用いて行う。また、ＬＡＮスイッチ１００の各ネットワークインターフェースＣ１０２～Ｆ１０７の設定は、ネットワークインターフェースＢ１０３は常に「接続状態」、ネットワークインターフェースＡ１０２は「状態なし」にそれぞれ設定し、ネットワークインターフェースＣ１０４～Ｆ１０７は特に設定をしない。したがって、ネットワークインターフェースＣ１０４～Ｆ１０７は、初期化時に「非接続状態」となる（なお、この際、ＬＡＮスイッチ１００の学習テーブル１０８は、図３に示すようになっている。）。

【００４６】つぎに、このネットワークシステムにおいて、ユーザ端末４０３（ＭＡＣアドレス２２：２２：ＦＦ：００：００：０１）がネットワークインターフェースＣ１０４につながる情報コンセント４０９に接続された場合について説明する。

【００４７】図５は、ユーザがユーザ端末４０３を情報コンセント４０９に接続した場合の通信シーケンス図である。

【００４８】まず、認証を受けていないユーザ端末４０３が、ファイルサーバ４０２にアクセスする場合、ユーザ端末４０３から、宛先アドレスがファイルサーバ４０２のＭＡＣアドレス（２２：２２：００：２２：２２：２２）、かつ、送信元アドレスがユーザ端末４０３のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）であるファイルサーバ宛パケット５０１が送信される。ここで、パケット５０１を受信したＬＡＮスイッチ１００の中継処理を説明する。

【００４９】図６は、パケット受信に対するＬＡＮスイッチ１００の中継処理を示すフローチャートである。

【００５０】パケット５０１を受信したＬＡＮスイッチ１００のパケット中継部１０１は、学習テーブル１０８を参照する。パケット５０１に含まれた送信元アドレス（ユーザ端末４０３のＭＡＣアドレス２２：２２：ＦＦ：００：００：０１）が学習テーブル１０８に登録されていなければ、パケット中継部１０１は、そのＭＡＣアドレスを学習テーブル１０８の１つのエントリにおけるアドレスフィールド３０１に登録する。また、パケット中継部１０１は、パケット５０１を受信したネットワークインターフェースの名前Ｃを送信ポートフィールド３０２に登録する。

【００５１】図７は、アドレス学習テーブル１０８の構成図（２）である。

【００５２】学習テーブル１０８のエントリ＃４におけるアドレスフィールドには、上述のように送信元アドレスとして、ユーザ端末４０３のＭＡＣアドレスが登録され、送信ポートフィールドには、ネットワークインターフェースＣが登録される。

【００５３】つぎに、パケット中継部１０１は、宛先アドレスであるファイルサーバ４０２のＭＡＣアドレス（２２：２２：００：２２：２２：２２）が学習テーブル１０８に登録済みであるので（処理６０２）、学習テーブル１０８のうちのファイルサーバ４０２の宛先アドレスが登録されているエントリの送信ポートフィールド３０２の内容に基づいて、パケット５０１を送信すべきポートとしてネットワークインターフェースＢの情報を取得する（処理６０３）。そしてパケット中継部１０１

は、パケット５０１の中継処理を行う（処理６０４）。

【００５４】ここで、処理６０４について説明する。

【００５５】図８は、処理６０４のフローチャートである。

【００５６】まず、パケット中継部１０１は、送信ポート（この場合ネットワークインターフェースＢ１０３）と受信ポート（この場合ネットワークインターフェースＣ１０４）とが同一かどうかを判定する（処理８０１）。ここでは、送信ポートと受信ポートは異なるポートであるので、後述する中継テーブル９０１に基づいて、パケット中継部１０１はパケット中継を行う（処理８０２）。

【００５７】図９は、中継テーブル９０１の構成図である。

【００５８】中継テーブル９０１は、受信ポートの状態と送信ポートの状態に基づいて、パケットの中継／廃棄を判定するために使用されるテーブルである。ここでは、ユーザ端末４０３から送信されたパケット５０１を受信するＬＡＮスイッチ１００の受信ポート（ネットワークインターフェースＣ１０４）は「非接続状態」であり、送信ポート（ネットワークインターフェースＢ１０３）は「接続状態」であるので、中継テーブル９０１は「廃棄」を指示している。その結果、パケット５０１はパケット中継部１０１によって廃棄される。これにより、認証を受けていないユーザ端末４０３からのファイルサーバ４０２へのアクセスは回避されたことになる。

【００５９】続いて、ユーザ端末４０３が、認証サーバ４０１に認証サーバ宛パケット５０２を送信する場合について説明する。

【００６０】ユーザ端末４０３が、宛先アドレスが認証サーバ４０１のＭＡＣアドレス（２２：２２：００：１１：１１：１１）であり、かつ、送信元アドレスがユーザ端末４０３のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）であるパケット５０２を送信する。このパケット５０２を受信したＬＡＮスイッチ１００のパケット中継部１０１は、上述した図６に示されたフローチャートに従い中継処理を行う。

【００６１】まず、学習テーブル１０８には、前回のパケット５０１受信時、ユーザ端末４０３のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）が既に登録されているので、パケット中継部１０１は処理６０１を通過する。つぎに、宛先アドレスである認証サーバ４０１のＭＡＣアドレス（２２：２２：００：１１：１１：１１）が学習テーブル１０８に登録済みであるので（処理６０２）、学習テーブル１０８のうちの認証サーバ４０１の宛先アドレスが登録されているエントリの送信ポートフィールド３０２の内容に基づいて、パケット５０２を送信すべきポートとしてネットワークインターフェースＡの情報を取得する（処理６０３）。そしてパケット中継部１０１は、パケット５０２の中継処理を行う（処理６０４）。

【００６２】ここで、再び、図８及び図９を用いて処理６０４について説明する。

【００６３】まず、送信ポート（この場合はネットワークインターフェースＡ１０２）が受信ポート（この場合はネットワークインターフェースＣ１０４）とは異なるので（処理８０１）、処理８０２に進む。ここで、受信ポートであるネットワークインターフェースＣ１０４の状態は「非接続状態」、送信ポートであるネットワークインターフェースＡ１０２の状態は「状態なし」であるので、中継テーブル９０１は「中継」を示している。この結果、パケット５０２は、パケット中継部１０１によってネットワークインターフェースＡ１０２から認証サーバ４０１に中継される。

【００６４】さらに、認証サーバ４０１からユーザ端末４０３への応答のパケット５０３は、同様に中継処理される。この場合、パケット５０３の受信ポートであるネットワークインターフェースＡ１０２の状態が「状態なし」、送信ポートであるネットワークインターフェースＣ１０４の状態が「非接続状態」であるので、中継テーブル９０１は「中継」を示す。従って、パケット５０３は、パケット中継部１０１によってネットワークインターフェースＣ１０４からユーザ端末４０３に中継される。つまり、認証サーバ４０１とユーザ端末４０３との間で双方向の通信が成立することになり、ユーザの認証が行われる。

【００６５】認証サーバ４０１では、例えば、ユーザ端末４０３から送られてきたパケット５０２に含まれているユーザＩＤ及びパスワード５０４が、ネットワークの使用許可を与えられたユーザのものと一致した場合、ＬＡＮスイッチ１００に対して接続許可を通知する。この接続許可の通知には、宛先アドレスがＬＡＮスイッチ１００のＭＡＣアドレス（２２：２２：００：ＦＦ：ＦＦ：ＦＦ）である状態変更指示パケット５０５が使用される。パケット５０５には、「接続状態への状態変更」とユーザ端末４０３のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）が情報として含まれている。

【００６６】状態変更指示パケット５０５を受信したＬＡＮスイッチ１００のパケット中継部１０１は、学習テーブル１０８を参照する。学習テーブル１０８において、状態変更指示パケット５０５の宛先アドレスであるＬＡＮスイッチ１００自身のＭＡＣアドレスが登録されているエントリ中の送信ポートフィールド３０２は「Ｘ」を示している（処理６０２）。従って、パケット５０５は、パケット中継部１０１により状態変更指示パケット処理部１０９に送られる（処理６０５）。状態変更指示パケット処理部１０９は、パケット５０５に含まれる情報からユーザ端末４０３のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）を取得すると共に、このＭＡＣアドレスを学習テーブル１０８のアドレ

スフィールド３０１から検索する。この検索によって得られた、ユーザ端末４０３のMACアドレスが登録されているエントリの送信ポートフィールド３０２に示されたネットワークインターフェース（この場合はC）に対して、状態変更指示パケット処理部１０９は、状態を「接続状態」に変更するように指示する。

【００６７】ネットワークインターフェースＣ１０４においては、状態管理部２０３が状態を「非接続状態」から「接続状態」に変更する。この結果、ユーザ端末４０３からファイルサーバ宛パケット５０６を送信する場合、受信ポートとなるネットワークインターフェースＣ１０４が「接続状態」となる。この場合、送信ポートとなるネットワークインターフェースＢ１０３が「接続状態」であるため、中継テーブル９０１は「中継」を示す。これにより、ユーザ端末４０３からファイルサーバ４０２へのアクセスが可能となる。

【００６８】次に、ユーザ端末４０３が情報コンセント４０９から離脱した場合のＬＡＮスイッチ１００の動作を説明する。

【００６９】ユーザが情報コンセント４０９からケーブル（ツイストペア線）を抜いてユーザ端末４０３の接続を解除すると、ネットワークインターフェースＣ１０４の物理インターフェース２０１が回線断の状態になる。その状態で１００ｍｓが経過すると、回線断検出部２０２は、状態管理部２０３に回線断を通知する。回線断を通知された状態管理部２０３は、ネットワークインターフェースＣ１０４の状態を「非接続状態」に変更する。これにより、新たなユーザ端末が同じ情報コンセント４０９に接続された場合でも、あらためて認証を受けるまではそのユーザ端末はファイルサーバ４０２にアクセスできなくなる。

【００７０】以上のように、本実施の形態のＬＡＮスイッチ１００を用いることで、認証前のユーザ端末４０３からは、ファイルサーバ４０２へのアクセスが阻止され、認証後はアクセスが可能になり、さらに、ユーザ端末４０３の離脱後は、他のユーザ端末が再び認証を行うまではファイルサーバ４０２へのアクセスが阻止されるネットワークシステムを構築することができる。また、本実施の形態では、ユーザ端末４０３がネットワークインターフェースＣ１０４につながる情報コンセント４０９に接続された場合について説明したが、ネットワークインターフェースＣ１０４～Ｆ１０７の動作は同様であり、ユーザ端末４０３が任意の情報コンセント４０９に接続されても同様の効果が得られる。

【００７１】また、本実施の形態では、ネットワークインターフェースの状態が、回線断により「非接続状態」に再初期化される。しかし、ユーザが離脱前に認証サーバ４０１と通信して離脱を通知し、その通知を受けた認証サーバ４０１が、「非接続状態に状態変更」を示す情報とユーザ端末４０３のMACアドレスとを含むパケットを、ＬＡＮスイッチ１００のMACアドレス（２２：２２：００：ＦＦ：ＦＦ：ＦＦ）宛に送り、そのパケットを受信した状態変更指示パケット処理部１０９の指示により、ネットワークインターフェースの状態が「非接続状態」に変更されても構わない。この構成によれば、ユーザは、ユーザ端末４０３と情報コンセント４０９の接続を切らずに、ネットワークの使用可否を制御できる。　図１０は、パケット通信装置の他の構成を示す図である。

【００７２】ルータ１０００は、例えば、複数の物理インターフェース１００２～１００７、パケット中継部１００１、複数のフィルタリング処理部１０１２～１０１７及びフィルタリング変更指示処理部１００９を備える。物理インターフェース１００２～１００７は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。パケット中継部１００１は、ＩＰ(Internet Protocol)プロトコルに基づいたパケット中継を行う。なお、本実施の形態では、パケット中継のプロトコルとしてＩＰプロトコル（ＩＰｖ４(ＩＰ version 4)）を用いるが、本発明は、例えば、ＩＰｖ６(ＩＰ version 6)など、その他のネットワーク層プロトコルにも適用可能である。また、本実施の形態では、パケット通信装置としてルータ１０００を使用しているが、ＬＡＮスイッチ等その他のパケット通信装置に対しても、本発明は適用可能である。

【００７３】図１１は、フィルタリング処理部１０１２～１０１７の構成図である。

【００７４】フィルタリング処理部１０１２～１０１７は、フィルタリングテーブル１１０１、パケット処理部１１０２を備える。フィルタリングテーブル１１０１には、パケットの中継または廃棄の判断のための情報が格納されている。パケット処理部１１０２は、フィルタリングテーブル１１０１の情報に基づいて、パケットの廃棄又は、パケット中継部１００１への送信を行う。パケット中継部１００１に送られたパケットは、物理インターフェース１００２～１００７に送信される。各フィルタリングテーブル１１０１は、フィルタリング変更指示処理部１００９と接続されており、フィルタリング変更指示処理部１００９からの指示に応じてフィルタリングテーブル１１０１の内容を変更することができる。

【００７５】図１２は、フィルタリングテーブル１１０１の構成図（１）である。

【００７６】フィルタリングテーブル１１０１は、パケットの中継または廃棄の判断のための情報を格納しており、各エントリは、宛先アドレス条件フィールド１２０１、送信元アドレス条件フィールド１２０２、中継／廃棄フラグフィールド１２０３を含む。宛先アドレス条件フィールド１２０１及び送信元アドレス条件フィールド１２０２には、ＩＰアドレスまたは「任意」を意味する情報が登録されている。中継／廃棄フラグフィールド１

２０３には、パケットの宛先アドレスと送信元アドレスがそれぞれ宛先アドレス条件と送信元アドレス条件に一致した受信パケットを中継すべきか又は廃棄すべきかを示す情報が登録されている。複数のエントリの情報と一致するパケットがあった場合は、テーブルの先頭に近いエントリがそのパケットに適用される。また、一致するエントリが一つもないパケットは、フィルタリング処理部によりパケット中継部１００１に送られる。

【００７７】フィルタリング変更指示処理部１００９は、後述される認証サーバ１３１１とネットワークを介して通信し、認証サーバ１３１１からフィルタリング変更指示を受ける。本実施の形態では、通信プロトコルとしてｔｅｌｎｅｔを想定するが、ＨＴＴＰやＣＯＰＳ（Common Open Policy Service）などのプロトコルが使用されてもよい。フィルタリング変更指示は、対象とするエントリの内容と、追加／削除の指示を含む。フィルタリング変更指示処理部１００９は、送信元アドレス条件フィールド１２０２に格納されているＩＰアドレスが属するサブネットに接続された物理インターフェース１００２～１００７に対応するフィルタリング処理部１０１２～１０１７のフィルタリングテーブル１１０１に、その指示を反映させる。

【００７８】図１３は、ルータ１０００を用いたネットワークシステムの構成図である。

【００７９】このネットワークシステムは、例えば、ルータ１０００の各物理インターフェース１００２～１００７にそれぞれ接続されているサブネットＡ１３０２～Ｆ１３０７と、サブネットＡ１３０２に接続されている認証サーバ１３１１と、サブネットＢ１３０３に接続されているファイルサーバ１３２２と、サブネットＣ１３０４～Ｆ１３０７にそれぞれ接続され、ユーザが自由に端末を接続できる複数の情報コンセント４０９と、情報コンセント４０１を介してサブネットＣ１３０４に接続されているユーザ端末１３３３とを含む。

【００８０】ルータ１０００のフィルタリング処理部Ａ１０１２、Ｂ１０１３における各フィルタリングテーブル１１０１には、初期状態では何も登録されていない。また、フィルタリング処理部Ｃ１０１４～Ｆ１０１７における各フィルタリングテーブル１１０１には、上述の図１２に示されている内容と同じ内容がそれぞれ設定されている。

【００８１】つぎに、このネットワークシステムで、ユーザ端末１３３３がサブネットＣ１３０４に接続された情報コンセント４０９に接続された場合について説明する。

【００８２】図１４は、ユーザによってユーザ端末１３３３が情報コンセント４０９に接続された場合の通信シーケンス図である。

【００８３】認証を受けていないユーザ端末１３３３は、ファイルサーバ１３２２にアクセスするため、ファイルサーバ１３２２のＩＰアドレス（１９２．１６８．２．２）宛のファイルサーバ宛パケット１４０１を送信する。この場合、パケット１４０１は、ルータ１０００の物理インターフェースＣ１００４を介して、フィルタリング処理部Ｃ１０１４に送られる。図１２に示されている通り、フィルタリング処理部Ｃ１０１４のフィルタリングテーブル１１０１のうち、宛先アドレス条件フィールド１２０１の内容が、パケット１４０１に含まれる宛先アドレスに該当するエントリは＃２のエントリである。フィルタリング処理部Ｃ１０１４は、フィルタリングテーブル１１０１の＃２のエントリを参照し、送信元アドレス条件フィールド１２０２や中継／排気フラグフィールド１２０３の内容を確認する。フィルタリングテーブル１１０１の＃２のエントリ中の中継／排気フラグフィールド１２０３の内容は「廃棄」を示している。従って、フィルタリング処理部Ｃ１０１４は、フィルタリングテーブル１１０１の内容に従ってパケット１４０１を廃棄する。よって、認証を受けていないユーザ端末１３３３の送信するパケット１４０１は、ファイルサーバ１３２２に到達することはない。

【００８４】つぎに、ユーザ端末１３３３が認証を受けてファイルサーバ１３２２にアクセスする場合の動作を説明する。

【００８５】ユーザ端末１３３３は、認証を受けるために、認証サーバ１３１１のＩＰアドレス（１９２．１６８．１．１）宛のパケット１４０２を送信する。パケット１４０２は、ルータ１０００の物理インターフェースＣ１００４で受信され、フィルタリング処理部Ｃ１０１４に送られる。フィルタリング処理部Ｃ１０１４は、パケット１４０２に対して、フィルタリングテーブル１１０１の検索を行う。この場合、フィルタリングテーブル１１０１のエントリのうち＃１、＃２の両方のエントリの宛先アドレス条件フィールド１２０１の内容が、パケット１４０１に含まれる宛先アドレスに該当する。そこで、テーブル内の先頭に登録されている＃１のエントリがパケット１４０２に適用される。フィルタリングテーブル１１０１の＃１のエントリ中の中継／排気フラグフィールド１２０３の内容は「中継」を示している。このため、フィルタリングテーブル１１０１の＃１のエントリを参照したフィルタリング処理部Ｃ１０１４は、中継／排気フラグフィールド１２０３の内容に従い、パケット１４０２をパケット中継部１００１に送る。パケット１４０２は、パケット中継部１００１によって物理インターフェースＡ１００２から認証サーバ１３１１に中継される。これによって、ユーザ端末１３３３から認証サーバ１３１１への通信が成立する。

【００８６】認証サーバ１３１１からユーザ端末１３３３へ送信された応答パケット１４０３は、物理インターフェースＡ１００２により受信され、フィルタリング処理部Ａ１０１２に送られる。フィルタリング処理部Ａ１

０１２のフィルタリングテーブル１１０１には何も登録されていない。従って、パケット１４０３はフィルタリング処理部Ａ１０１２からパケット中継部１００１に送られる。パケット中継部１００１は、物理インターフェースＣ１００４からパケット１４０３をユーザ端末１３３３に送信する。これによって、ユーザ端末１３３３と認証サーバ１３１１との双方向の通信が成立することになり、ユーザ端末１３３３は、認証サーバ１３１１から認証を受けることができる。

【００８７】パケット１４０３は、ユーザ端末１４３３に対してユーザＩＤ及びパスワードの送信を要求する。従って、パケット１４０３を受信したユーザ端末１３３３に対してユーザはユーザＩＤ及びパスワードを入力する。入力されたユーザＩＤとパスワードを含むパケット１４０４が、ユーザ端末１３３３から認証サーバ１３１１に送られる。パケット１４０４は、上述のようにしてルータ１０００により中継され、認証サーバ１３１１に受信される。認証サーバ１３１１は、ユーザ端末１３３３から送られてきたパケット１４０４に含まれるユーザＩＤとパスワードが、ネットワーク接続を許可されたユーザのものと一致した場合、ルータ１０００のフィルタリング変更指示処理部１００９と通信し、フィルタリングテーブル１１０１に対して、宛先アドレス条件フィールド１２０１の内容が「任意」、送信元アドレス条件フィールド１２０２の内容がユーザ端末１３３３のＩＰアドレスである「１９２．１６８．３．３」、中継／廃棄フラグフィールド１２０３の内容が「中継」であるエントリを追加することを指示１４０５する。

【００８８】図１５は、フィルタリングテーブル１１０１の構成図（２）である。

【００８９】フィルタリング変更指示処理部１００９は、認証サーバ１３１１から指示された送信元アドレス条件「１９２．１６８．３．３」が属するサブネット（サブネットＣ１３０４）が物理インターフェースＣ１００４に接続されている為、フィルタリング処理部Ｃ１０１４のフィルタリングテーブル１１０１に対して、指示されたエントリを追加する。その結果、図１５に示されるように、フィルタリング処理部Ｃ１０１４のフィルタリングテーブル１１０１には、新たなエントリが＃１のエントリとして追加され、＃１～＃３までのエントリがフィルタリングテーブル１１０１に登録されていることになる。

【００９０】その後、ユーザ端末１３３３がファイルサーバ１３２２宛のパケット１４０６を送信した場合、パケット１４０６に含まれる送信元アドレスがフィルタリング処理部Ｃ１０１４のフィルタリングテーブル１１０１における＃１のエントリの送信元アドレス条件に該当する。このため、パケット１４０６はフィルタリング処理部Ｃ１０１４からパケット中継部１００１に送られ、ファイルサーバ１３２２に中継される。この結果、ユーザ端末１３３３からファイルサーバ１３２２へのアクセスが可能となる。

【００９１】以上のように、ルータ１０００を用いることで、認証サーバ１３１１による認証を受けていないユーザ端末１３３３からファイルサーバ１３２２へのアクセスは阻止され、ユーザ端末１３３３が認証を受けた後、ユーザ端末１３３３からファイルサーバ１３２２へのアクセスが許可されるネットワークシステムを構築することができる。また、ルータ１０００の各物理インターフェース１００２～１００７は複数の情報コンセント４０９を扱うことができる。さらに、物理インターフェースごとに個別のフィルタリング処理部が設けられることにより、ルータ１０００においてフィルタリング処理の負荷を分散することができる。

【００９２】図１６は、パケット通信装置の他の構成を示す図である。

【００９３】ＬＡＮスイッチ１６００は、例えば、パケット中継部１６０１、複数のネットワークインターフェース１６０２～１６０５、アドレス学習テーブル１６０６、フィルタリングテーブル１６０７及び状態変更指示パケット処理部１６０８を備える。ネットワークインターフェース１６０２～１６０５には、各々を一意に識別するために名前（図ではＡ～Ｄ）が割り当てられている。なお、名前は、一意に識別できれば番号等であってもよい。

【００９４】これらのネットワークインターフェース１６０２～１６０５は、それぞれ異なるネットワークに接続されており、パケットの送受信を行う。なお、ネットワークは、ＩＥＥＥの８０２．３ネットワークである。また、以下の説明では、ネットワークインターフェースＡ１６０２を「アップリンク」、ネットワークインターフェースＢ１６０３～Ｄ１６０５を「ダウンリンク」と称する。

【００９５】パケット中継部１６０１は、アドレス学習テーブル１６０６とフィルタリングテーブル１６０７が保持する情報に基づいて、ネットワーク間でのパケット中継を行う。状態変更指示パケット処理部１６０８は、後述する認証サーバ１９０１からの状態変更指示パケットを受信し、フィルタリングテーブル１６０７と学習テーブル１６０６の内容を変更する。状態変更指示パケットには、ＩＰアドレスと「許可／禁止」を示す情報とが含まれる。

【００９６】図１７は、フィルタリングテーブル１６０７の構成図である。

【００９７】フィルタリングテーブル１６０７には、中継が許可されていないパケットを識別するための情報が登録されている。フィルタリングテーブル１６０７の各エントリは、ＭＡＣアドレスフィールド１７０１、ＩＰアドレスフィールド１７０２、接続ポートフィールド１７０３を含む。ＭＡＣアドレスフィールド１７０１に

は、フィルタリング対象となるＭＡＣアドレスが、ＩＰアドレスフィールド１７０２には、そのＭＡＣアドレスに対応するＩＰアドレスが、接続ポートフィールド１７０３には、そのＭＡＣアドレスを持つユーザ端末が属するネットワークに接続されているネットワークインターフェース１６０２～１６０５の名前が、それぞれ登録されている。

【００９８】図１８は、学習テーブル１６０６の構成図（１）である。

【００９９】学習テーブル１６０６には、パケットの中継先ネットワークインターフェースに関する情報が登録されている。学習テーブル１６０６の各エントリは、ＭＡＣアドレスフィールド１８０１及び接続ポートフィールド１８０２を含む。ＭＡＣアドレスフィールド１８０１には、中継対象となるＭＡＣアドレスが、接続ポートフィールド１８０２には、パケットに含まれる宛先ＭＡＣアドレスがＭＡＣアドレスフィールドの内容に一致したパケットを中継すべきネットワークインターフェース１６０２～１６０５の名前が、それぞれ登録されている。また、一定時間利用されなかったエントリは、自動的に学習テーブル１６０６から削除されるように設定されている。

【０１００】次に、図１９に示されたネットワークを例に、ＬＡＮスイッチ１６００を用いたネットワークシステムの動作を説明する。

【０１０１】図１９は、ＬＡＮスイッチ１６００を用いたネットワークシステムの構成図である。

【０１０２】このネットワークシステムは、例えば、ＬＡＮスイッチ１６００と、ＬＡＮスイッチ１６００の各ネットワークインターフェース１６０２～１６０５にそれぞれ接続されたネットワークＡ～Ｄと、ネットワークＢ～Ｄを介して、ダウンリンクの各ネットワークインターフェースＢ１６０３～Ｄ１６０５に接続された、ユーザが自由に端末を接続できる複数の情報コンセント４０９と、情報コンセント４０９を介してネットワークＢに接続されたユーザ端末１９０５と、ネットワークＡを介してアップリンクのネットワークインターフェースＡに接続されたルータ１９０４と、ネットワークを介してルータ１９０４に接続されたファイルサーバ１９０２、ＤＨＣＰサーバ１９０３、認証サーバ１９０１とを含む。

【０１０３】ルータ１９０４は、ＢＯＯＴＰリレーエージェント機能を備え、ＩＰプロトコルに基づいたパケットの中継を行う。ＤＨＣＰサーバ１９０３は、ＤＨＣＰプロトコルに基づきユーザ端末にＩＰアドレスを配布する。認証サーバ１９０１は、ユーザ認証の結果を状態変更指示パケットとしてＬＡＮスイッチ１６００に通知する。このネットワークシステムにおいて、各ネットワークに接続された機器には、そのネットワークに属するＩＰアドレスが割り当てられている（図中ＩＰアドレスと表記されたアドレス）。各ネットワークに接続された各機器のインターフェースには物理アドレス（以下ＭＡＣアドレスと記載する）が設定されている。以下の説明で必要となるＭＡＣアドレスは、図中に「ＭＡＣアドレス」と表記されている。

【０１０４】つぎに、ユーザ端末１９０５がネットワークＢの情報コンセント４０９に接続された場合について説明する。

【０１０５】図２０は、ユーザ端末１９０５がネットワークＢの情報コンセント４０９に接続された場合の通信シーケンス図である。

【０１０６】初期状態では、ＬＡＮスイッチ１６００のフィルタリングテーブル１６０７には、何も登録されていない。また、学習テーブル１６０６は、ＭＡＣアドレスフィールド１８０１にルータ１９０４のＭＡＣアドレス（２２：２２：００：４４：４４：４４）を、接続ポートフィールド１８０２にネットワークインターフェースＡ１６０２の名前をそれぞれ格納している１つのエントリを持っている。

【０１０７】まず、ユーザ端末１９０５は、情報コンセント４０９に接続されると、ＤＨＣＰプロトコルによりＩＰアドレスを要求するためのアドレス要求パケット２００１を送信する。この場合、ユーザ端末１９０５はパケット２００１の宛先アドレスをブロードキャストアドレスとして送信する。パケット２００１はＬＡＮスイッチ１６００のネットワークインターフェースＢ１６０３により受信され、パケット中継部１６０１に送られる。

【０１０８】パケット２００１を受信したＬＡＮスイッチ１６００の中継処理を説明する。

【０１０９】図２１は、パケット受信に対するＬＡＮスイッチ１６００のパケット中継部１６０１の中継処理を示すフローチャートである。

【０１１０】パケット２００１を受信するとパケット中継部１６０１は、パケット２００１の宛先アドレスが学習テーブル１６０６に登録されているか検索する（処理２１０１）。宛先アドレスは学習テーブル１６０６に登録されていない為、宛先アドレスがブロードキャストアドレスか判断する（処理２１０２）。宛先アドレスはブロードキャストアドレスである為、受信ポートがアップリンクか判断する（処理２１０３）。受信ポートはネットワークインターフェースＢ１６０３であってアップリンクではない為、パケット２００１の送信元アドレスが学習テーブル１６０６に登録されているか検索する（処理２１０４）。送信元アドレスであるユーザ端末１９０５のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）は学習テーブル１６０６に登録されていない。また、フィルタリングテーブル１６０７にもこの送信元アドレスは登録されていない為、パケット中継部１６０１はユーザ端末１９０５のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）をフィルタリングテーブル１６０７の１つのエントリのＭＡＣアドレスフィールド１

７０１に登録する（処理２１０５）。

【０１１１】この場合、図１７に示すように、フィルタリングテーブル１６０７のそのエントリのＩＰアドレスフィールド１７０２には「未登録」を示す情報、接続ポートフィールド１７０３にはネットワークインターフェースＢ１６０３の名前「Ｂ」がそれぞれ登録される。

【０１１２】そして、パケット中継部１６０１はパケット２００１をアップリンクにのみ中継し、ルータ１９０４に送る（処理２１０５）。

【０１１３】パケット２００１はアドレス要求パケットであるので、ルータ１９０４のＢＯＯＴＰリレーエージェント機能によってＤＨＣＰサーバ１９０３に中継される。

【０１１４】図２０において、ＤＨＣＰサーバ１９０３から送信されたアドレス配布パケット２００２は、ルータ１９０４のＢＯＯＴＰリレーエージェント機能により、ユーザ端末１９０５のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）宛に送られる。

【０１１５】パケット２００２はＬＡＮスイッチ１６００のネットワークインターフェースＡ１６０２により受信され、パケット中継部１６０１に送られる。パケット中継部１６０１は、図２１に示されたフローチャートに従ってパケット２００２を中継処理する。パケット中継部１６０１は、パケット２００２の宛先アドレスであるユーザ端末１９０５のＭＡＣアドレスが学習テーブル１６０６に登録されているか検索する（処理２１０１）。宛先アドレスは学習テーブル１６０６に登録されていない為、宛先アドレスがブロードキャストアドレスか判断する（処理２１０２）。宛先アドレスはブロードキャストアドレスではない為、宛先アドレスがフィルタリングテーブル１６０７に登録されているか検索する（処理２１０６）。フィルタリングテーブル１６０７にはユーザ端末１９０５のＭＡＣアドレスが登録されている為、受信ポートがアップリンクか判断する（処理２１０７）パケット２００２の受信ポートはネットワークインターフェースＡ１６０２であり、アップリンクである為、パケット２００２の通信プロトコルがＩＰプロトコルか判断する（処理２１０８）。通信プロトコルはＩＰプロトコルである為、パケット２００２に含まれる送信元ＩＰアドレスがリレーエージェント（ルータ１９０４）または認証サーバのＩＰアドレスか判断する（処理２１０９）。送信元ＩＰアドレスはリレーエージェント（ルータ１９０４）のＩＰアドレスである為、パケット中継部１６０１はパケット２００２を中継する。この場合、パケット中継部１６０１はパケット２００２の宛先アドレスがＭＡＣアドレスフィールド１７０１の内容と一致するフィルタリングテーブル１６０７のエントリ＃１を参照する。エントリ＃１の接続ポートフィールド１７０３にはネットワークインターフェースＢ１６０３の名前が登録されている為、パケット中継部１６０１は、パケット２００２をネットワークインターフェースＢ１６０３に中継し、ネットワークインターフェースＢ１６０３から送信させる（処理２１１０）。これによって、ユーザ端末１９０５にアドレス配布パケット２００２が送られる。ここで、ユーザ端末１９０５に、ＤＨＣＰサーバ１９０３から配布されたＩＰアドレスが「１９２．１６８．５．１」であるとする。

【０１１６】次に、ユーザ端末１９０５が認証サーバによる認証を受けずにファイルサーバ１９０２にアクセスを試みる場合について説明する。但し、アクセスのためのプロトコルとしてはＩＰが用いられる。

【０１１７】図１９に示されたネットワークシステムにおいて、ファイルサーバ１９０２（ＩＰアドレス１９２．１６８．１．２）とユーザ端末１９０５（ＩＰアドレス１９２．１６８．５．１）は、それぞれが接続しているサブネットが異なる。その為、ユーザ端末１９０５がファイルサーバ１９０２にアクセスするために送信するパケット２００３は、宛先ＩＰアドレスとしてファイルサーバ１９０２のＩＰアドレス（１９２．１６８．１．２）を含み、宛先ＭＡＣアドレスとしてルータ１９０４のＭＡＣアドレス（２２：２２：００：４４：４４：４４）を含む。パケット２００３はユーザ端末１９０５から送信され、ＬＡＮスイッチ１６００のネットワークインターフェースＢ１６０３に受信される。ネットワークインターフェースＢは受信したパケット２００３をパケット中継部１６０１に送る。

【０１１８】パケット２００３を受信したＬＡＮスイッチ１６００のパケット中継部１６０１の処理を図２１に示されたフローチャートを用いて説明する。

【０１１９】パケット２００３を受信するとパケット中継部１６０１は、パケット２００３の宛先ＭＡＣアドレスが学習テーブル１６０６に登録されているか検索する（処理２１０１）。宛先ＭＡＣアドレスであるルータ１９０４のＭＡＣアドレスは学習テーブル１６０６に登録されている。従って、パケット中継部１６０１は、パケット２００３の通信プロトコルがＩＰプロトコルであるか、また、パケット２００３に含まれる送信元ＭＡＣアドレスがフィルタリングテーブル１６０７に登録されているかを確認する（処理２１１１）。パケット２００３の通信プロトコルはＩＰプロトコルであり、また、送信元ＭＡＣアドレスであるユーザ端末１９０５のＭＡＣアドレスはフィルタリングテーブル１６０７に登録されている。従って、パケット中継部１６０１は、フィルタリングテーブル１６０７のうちのユーザ端末１９０５のＭＡＣアドレスが登録されているエントリにおけるＩＰアドレスフィールド１７０２に、パケット２００３に含まれる送信元ＩＰアドレスを登録する（処理２１１１）。この場合、図１７に示されるように、フィルタリングテーブル１６０７のうちのユーザ端末１９０５のＭＡＣアドレスが登録されているエントリにおけるＩＰアドレス

フィールド１７０２には「未登録」を示す情報が元々登録されている為、その情報がパケット２００３に含まれる送信元ＩＰアドレスに変更されることになる。尚、パケット２００３に含まれる送信元ＩＰアドレスは、ＤＨＣＰサーバ１９０３からユーザ端末１９０５に配布されたＩＰアドレス（１９２．１６８．５．１）である。

【０１２０】その後、パケット中継部１６０１は、学習テーブル１６０６のうちの宛先ＭＡＣアドレスが登録されたエントリにおける接続ポートフィールド１８０２の内容に従って、パケット２００３をアップリンクに中継する。パケット２００３はアップリンクからルータ１９０４に送られる。パケット２００３はＩＰプロトコルの仕様に基づいてルータ１９０４によってファイルサーバ１９０２に中継される。

【０１２１】ファイルサーバ１９０２は、パケット２００３を受信すると、ユーザ端末１９０５によって要求されたデータを含むパケット２００４を、応答パケットとして送信する。パケット２００４はルータ１９０４に受信され、中継されてＬＡＮスイッチ１６００に送られる。ＬＡＮスイッチ１６００のネットワークインターフェースＡ１６０２はパケット２００４を受信し、パケット中継部１６０１に送る。

【０１２２】次に、パケット２００４を受信したＬＡＮスイッチ１６００のパケット中継部１６０１の処理について図２１に示されたフローチャートに従って説明する。

【０１２３】まず、パケット２００４は宛先ＭＡＣアドレスとしてユーザ端末１９０５のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）、宛先ＩＰアドレスとしてユーザ端末１９０５のＩＰアドレス（１９２．１６８．５．１）、送信元ＩＰアドレスとしてファイルサーバ１９０２のＩＰアドレス（１９２．１６８．１．２）を含む。

【０１２４】パケット中継部１６０１は、パケット２００４の宛先ＭＡＣアドレスであるユーザ端末１９０５のＭＡＣアドレスが学習テーブル１６０６に登録されているか検索する（処理２１０１）。宛先ＭＡＣアドレスは学習テーブル１６０６に登録されていない為、宛先ＭＡＣアドレスがブロードキャストアドレスか判断する（処理２１０２）。宛先ＭＡＣアドレスはブロードキャストアドレスではない為、宛先ＭＡＣアドレスがフィルタリングテーブル１６０７に登録されているか検索する（処理２１０６）。フィルタリングテーブル１６０７にはユーザ端末１９０５のＭＡＣアドレスが登録されている為、受信ポートがアップリンクか判断する（処理２１０７）パケット２００４の受信ポートはネットワークインターフェースＡ１６０２であり、アップリンクである為、パケット２００４の通信プロトコルがＩＰプロトコルか判断する（処理２１０８）。通信プロトコルはＩＰプロトコルである為、パケット２００４に含まれる送信元ＩＰアドレスがリレーエージェント（ルータ１９０４）または認証サーバのＩＰアドレスか判断する（処理２１０９）。送信元ＩＰアドレスはファイルサーバ１９０２のＩＰアドレスである為、パケット２００４を廃棄する（処理２１０９）。即ち、パケット２００４はＬＡＮスイッチ１６００からユーザ端末１９０５に送信されない。従って、ユーザ端末１９０５からファイルサーバ１９０２へのアクセスは成立しない。

【０１２５】次に、ユーザ端末１９０５が認証サーバ１９０１から認証を受ける場合について説明する。

【０１２６】ユーザは、認証サーバ１９０１による認証を受ける為、ユーザ端末１９０５にユーザＩＤ及びパスワードを入力する。ユーザ端末１９０５は、入力されたユーザＩＤとパスワードを含むパケット２００５を認証サーバ１９０１宛に送信する。この場合において、認証サーバ（ＩＰアドレス１９２．１６８．１．１）とユーザ端末１９０５（ＩＰアドレス１９２．１６８．５．１）のそれぞれが属するサブネットは異なる。その為、パケット２００５は、宛先ＩＰアドレスとして認証サーバ１９０１のＩＰアドレス（１９２．１６８．１．１）を含み、宛先ＭＡＣアドレスとしてルータ１９０４のＭＡＣアドレス（２２：２２：００：４４：４４：４４）を含む。パケット２００５はユーザ端末１９０５から送信され、ＬＡＮスイッチ１６００のネットワークインターフェースＢ１６０３に受信される。ネットワークインターフェースＢは受信したパケット２００５をパケット中継部１６０１に送る。

【０１２７】パケット２００５を受信したＬＡＮスイッチ１６００のパケット中継部１６０１の処理を図２１に示されたフローチャートを用いて説明する。

【０１２８】パケット２００５を受信するとパケット中継部１６０１は、パケット２００５の宛先ＭＡＣアドレスが学習テーブル１６０６に登録されているか検索する（処理２１０１）。宛先ＭＡＣアドレスであるルータ１９０４のＭＡＣアドレスは学習テーブル１６０６に登録されている。従って、パケット中継部１６０１は、パケット２００５の通信プロトコルがＩＰプロトコルであるか、また、パケット２００５に含まれる送信元ＭＡＣアドレスがフィルタリングテーブル１６０７に登録されているかを確認する（処理２１１１）。パケット２００５の通信プロトコルはＩＰプロトコルであり、また、送信元ＭＡＣアドレスであるユーザ端末１９０５のＭＡＣアドレスはフィルタリングテーブル１６０７に登録されている。更に、パケット２００５に含まれる送信元ＩＰアドレスもフィルタリングテーブル１６０７に登録されている。従って、パケット中継部１６０１は、学習テーブル１６０６のうちの宛先ＭＡＣアドレスが登録されたエントリにおける接続ポートフィールド１８０２の内容に従って、パケット２００５をアップリンクに中継する。パケット２００５はアップリンクからルータ１９０４に

送られる。パケット２００５はＩＰプロトコルの仕様に基づいてルータ１９０４によって認証サーバ１９０１に中継される。

【０１２９】認証サーバ１９０１は、ユーザ端末１９０５から送られたパケット２００５に含まれるユーザＩＤとパスワードが、ネットワークの使用を許可されたユーザのものであった場合、状態変更指示通知パケット２００６をＬＡＮスイッチ１６００の状態変更指示通知パケット処理部１６０８宛に送信する。この状態変更指示通知パケット２００６は、ユーザ端末１９０５のＩＰアドレス（１９２．１６８．５．１）と「許可」を示す情報を含む。状態変更指示通知パケット２００６は、ルータ１９０４によってＬＡＮスイッチ１６００に中継される。ＬＡＮスイッチ１６００のネットワークインターフェースＡ１６０２は状態変更指示通知パケット２００６を受信し、パケット中継部１６０１を介して状態変更指示通知パケット処理部１６０８に送る。状態変更指示通知パケット処理部１６０８は、状態変更指示通知パケット２００６を受けて、状態変更指示通知パケット２００６に含まれるＩＰアドレス（１９２．１６８．５．１）をフィルタリングテーブル１６０７から検索する。状態変更指示通知パケット処理部１６０８は、フィルタリングテーブル１６０７からＩＰアドレス（１９２．１６８．５．１）が登録されているエントリを見つけ、そのエントリのＭＡＣアドレスフィールド１７０１と接続ポートフィールド１７０３から、ＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）と接続ポートの名前（Ｂ）を読み出す。状態変更指示通知パケット処理部１６０８は、読み出したＭＡＣアドレスと接続ポートの名前が登録された新たなエントリを学習テーブル１６０６に追加する。

【０１３０】図２２は、学習テーブル１６０６の構成図（２）である。図２２に示されるように、学習テーブル２２は、＃２のエントリとしてＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）と接続ポートの名前（Ｂ）を含むエントリを持つ。

【０１３１】認証サーバ１９０１の認証後、ユーザ端末１９０５が再度ファイルサーバ１９０２にアクセスする為にパケット２００７を送信すると、上述と同様に、パケット２００７は、ＬＡＮスイッチ１６０２及びルータ１９０４によって中継されてファイルサーバ１９０２に送られる。

【０１３２】ファイルサーバ１９０２は、パケット２００７を受信すると、ユーザ端末１９０５によって要求されたデータを含むパケット２００８を、応答パケットとして送信する。パケット２００８はルータ１９０４に受信され、中継されてＬＡＮスイッチ１６００に送られる。ＬＡＮスイッチ１６００のネットワークインターフェースＡ１６０２はパケット２００８を受信し、パケット中継部１６０１に送る。パケット２００８を受信したパケット中継部１６０１は、図２１に示されたフローチャートに従って次のように処理する。

【０１３３】パケット２００８は宛先ＭＡＣアドレスとしてユーザ端末１９０５のＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）、宛先ＩＰアドレスとしてユーザ端末１９０５のＩＰアドレス（１９２．１６８．５．１）、送信元ＩＰアドレスとしてファイルサーバ１９０２のＩＰアドレス（１９２．１６８．１．２）を含む。

【０１３４】パケット中継部１６０１は、パケット２００８の宛先ＭＡＣアドレスであるユーザ端末１９０５のＭＡＣアドレスが学習テーブル１６０６に登録されているか検索する（処理２１０１）。宛先ＭＡＣアドレスはユーザ端末１９０５のＭＡＣアドレス（２２；２２：ＦＦ：００：００：０１）であるので、図２２に示されるように学習テーブル１６０６に登録されている。従って、パケット中継部１６０１は、パケット２００８の通信プロトコルがＩＰプロトコルであるか、また、パケット２００８に含まれる送信元ＭＡＣアドレスがフィルタリングテーブル１６０７に登録されているかを確認する（処理２１１１）。パケット２００８の通信プロトコルはＩＰプロトコルであり、また、送信元ＭＡＣアドレスであるルータ１９０４のＭＡＣアドレスはフィルタリングテーブル１６０７に登録されていない為、フィルタリングテーブル１６０７には何も登録しない。そして、パケット中継部１６０１は、学習テーブル１６０６のうちの宛先ＭＡＣアドレスが登録されたエントリにおける接続ポートフィールド１８０２の内容に従って、パケット２００８をネットワークインターフェースＢ１６０３に中継する。パケット２００８はネットワークインターフェースＢ１６０３からユーザ端末１９０５に送られる。これにより、ユーザ端末１９０５からファイルサーバ１９０２へのアクセスが成立する。

【０１３５】認証を受けた後、ユーザ端末１９０５が一定時間ファイルサーバと通信をしなかった場合、学習テーブル１６０６のエントリ（エントリ＃２）は自動的に削除される。従って、再びユーザ端末１９０５が認証サーバによる認証を受けるまではファイルサーバ１９０２へのアクセスはできなくなる。また、ＤＨＣＰサーバ１９０３によるアドレス配布において、通常、配布されたアドレスの使用期限が設けられている。このため、ＤＨＣＰサーバ１９０３は、ユーザ端末１９０５にアドレス配布を行ってから所定の時間が経過し、アドレスの使用期限が過ぎたら、タイムアウト通知２００９を認証サーバ１９０１に対して行う。タイムアウト通知２００９を受けた認証サーバは、使用期限の過ぎたＩＰアドレス（この場合１９２．１６８．５．１）、および「禁止」という情報を含む状態変更指示通知パケット２０１０をＬＡＮスイッチ１６００の状態変更指示通知パケット処理部１６０８宛に送信する。状態変更指示通知パケット

２０１０は、ルータ１９０４によってＬＡＮスイッチ１６００に中継される。ＬＡＮスイッチ１６００のネットワークインターフェースＡ１６０２は状態変更指示通知パケット２０１０を受信し、パケット中継部１６０１を介して状態変更指示通知パケット処理部１６０８に送る。状態変更指示通知パケット処理部１６０８は、状態変更指示通知パケット２０１０を受けて、状態変更指示通知パケット２０１０に含まれるＩＰアドレス（１９２．１６８．５．１）をフィルタリングテーブル１６０７から検索する。状態変更指示通知パケット処理部１６０８は、フィルタリングテーブル１６０７からＩＰアドレス（１９２．１６８．５．１）が登録されているエントリを見つけ、そのエントリのＭＡＣアドレスフィールド１７０１から、ＭＡＣアドレス（２２：２２：ＦＦ：００：００：０１）を読み出す。状態変更指示通知パケット処理部１６０８は、更に、読み出したＭＡＣアドレスを学習テーブル１６０６から検索し、そのＭＡＣアドレスが登録されているエントリを見つける。状態変更指示通知パケット処理部１６０８は、フィルタリングテーブル１６０７と学習テーブル１６０６の双方から、見つけたエントリをそれぞれ削除する。その結果、ユーザ端末１９０５は、再び認証を受けない限りファイルサーバ１９０２にアクセスできなくなる。

【０１３６】以上のように、ＬＡＮスイッチ１６００を用いることで、認証を受けていないユーザ端末１９０５からのファイルサーバ１９０２へのアクセスが防止され、認証を受けたユーザ端末１９０５からのファイルサーバ１９０２へのアクセスが許可されるネットワークシステムを構築できる。また、情報コンセントに接続されたユーザ端末が一定時間無通信である場合や、ユーザ端末に配布されたアドレスの使用期限が過ぎた場合に、ＬＡＮスイッチ１６００内のテーブルを自動的に変更し、再びユーザ端末が認証を受けるまではファイルサーバ１９０２へのアクセスを防止することもできる。

【０１３７】図２３は、パケット通信装置としてルータ２３００を用いたネットワークシステムの構成図である。

【０１３８】ルータ２３００は、例えば、複数のネットワークインターフェースＡ２３０２～Ｄ２３０５、パケット中継部２３０１、ＩＰアドレス登録表２３０６を備える。

【０１３９】パケット中継部２３０１は、ＩＰプロトコルに基づいてパケット中継を行う。また、パケット中継部２３０１はＩＰアドレス登録表２３０６に登録されていないＩＰアドレスを持つユーザ端末からのパケットに対して、カプセル化処理を行う。ネットワークインターフェースＡ２３０２～Ｄ２３０５は、それぞれ異なるネットワークに接続され、パケットの送受信を行う。ＩＰアドレス登録表２３０６には、認証を受けたユーザ端末のＩＰアドレスが登録される。

【０１４０】また、このネットワークシステムは、例えば、ルータ２３００と、ルータ２３００のネットワークインターフェースＡ２３０２に、ネットワークＡを介して接続された認証サーバ２３１０及びファイルサーバ２３１１と、ネットワークインターフェースＢ２３０３～Ｄ２３０５に、ネットワークＢ～Ｄをそれぞれ介して接続され、ユーザが端末を自由に接続できる複数の情報コンセント４０９と、情報コンセント４０９を介してネットワークＢ２３１３に接続されたユーザ端末２３１２とを含む。認証サーバ２３１０は、ユーザ認証を行うと共に、その結果をルータ２３００に通知し、後述するカプセル化されたパケットの送受信を行う。

【０１４１】つぎに、このネットワークシステムにおいて、ユーザ端末２３１２がネットワークＢ２３１３に接続された情報コンセント４０９に接続された場合について説明する。

【０１４２】図２７は、初期状態でのＩＰアドレス登録表２３０６の構成図である。図２４は、ユーザによってユーザ端末２３１２が情報コンセント４０９に接続された場合の通信シーケンス図である。

【０１４３】ユーザ端末２３１２が認証サーバ２３１０による認証を受けずにファイルサーバ２３１１へのアクセスを試みた場合について説明する。

【０１４４】認証を受けていないユーザ端末２３１２は、ファイルサーバ２３１１にアクセスするため、ファイルサーバ２３１１のＩＰアドレス（１９２．１６８．１０．２）宛のパケット２４００を送信する。この場合、パケット２４００は、ルータ２３００のネットワークインターフェースＢ２３０３に受信され、パケット中継部２３０１に送られる。パケット中継部２３０１は、ユーザ端末２３１２からのパケット２４００を受信し、中継処理を行う。

【０１４５】図２５は、ルータ２３００のパケット中継装置２３０１の中継処理を示すフローチャートである。

【０１４６】パケット２４００を受信すると、パケット中継部２３０１は、パケット２４００の宛先アドレスがルータ２３００のカプセル化用アドレスか判断する（処理２５０１）。パケット２４００の宛先アドレスは、ファイルサーバ２３１１のＩＰアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット２４００の送信元アドレスがＩＰアドレス登録表２３０６に登録されているか検索する（処理２５０２）。送信元アドレスであるユーザ端末２３１２のＩＰアドレスはＩＰアドレス登録表２３０６に登録されていない為、パケット中継部２３０１は、パケット２４００をカプセル化する（処理２５０３）。

【０１４７】ここで、「カプセル化」とは、ＩＰヘッダを含むパケット２４００全体を１つのデータとみなし、このデータに対して、宛先アドレスとして認証サーバ２３１０のカプセル化用アドレス（１９２．１６８．１０

０．１００）、送信元アドレスとしてルータ２３００のカプセル化用アドレス（１９２．１６８．１００．１０１）を含むＩＰヘッダを付加することにより、新たなパケット（カプセル化したパケット）を作成することである。この為、カプセル化したパケットは、元々の宛先アドレス（例えば、ファイルサーバ２３１１のＩＰアドレス）に係わらず、認証サーバ２３１０に送信されることになる（処理２５０４）。

【０１４８】ここで、カプセル化されたパケットを受信した認証サーバ２３１０の処理について説明する。

【０１４９】図２６は、パケットを受信した認証サーバ２３１０の処理を示すフローチャートである。

【０１５０】カプセル化されたパケットを受信した認証サーバ２３１０は、パケットの宛先アドレスが認証サーバのカプセル化用アドレスか判断する（処理２６０１）。カプセル化されたパケットの宛先アドレスは認証サーバのカプセル化アドレスである為、パケットの送信元アドレスがルータ２３００のカプセル化用アドレスであるか判断する（処理２６０２）。送信元アドレスはルータのカプセル化用アドレスである為、受信したパケットのカプセル化を解除し、元々のパケット２４００を復元する（処理２６０３）。カプセル化を解除するとは、カプセル化されたパケットからＩＰヘッダを取り除き、カプセル化されたパケットにデータとして含まれていたカプセル化される前のパケット２４００を取り出すことである。

【０１５１】次に、認証サーバ２３１０は、カプセル化を解除したパケット２４００の宛先アドレスが認証サーバのＩＰアドレスであるか判断する（処理２６０４）。パケット２４００の宛先アドレスはファイルサーバ２３１１のＩＰアドレスであって、認証サーバ２３１０のＩＰアドレスではない。従って、認証サーバ２３１０はパケット２４００を廃棄する。

【０１５２】この結果、認証を受けていないユーザ端末２３１２は、ファイルサーバ２３１１へアクセスすることはできない。

【０１５３】次に、ユーザ端末２３１２が認証サーバ２３１０から認証を受ける場合について図２４及び図２５を用いて説明する。

【０１５４】ユーザは、認証サーバ２３１０による認証を受ける為、ユーザ端末２３１２にユーザＩＤ及びパスワードを入力する。ユーザ端末２３１２は、入力されたユーザＩＤとパスワードを含むパケット２４０１を認証サーバ２３１０宛に送信する。パケット２４０１はルータ２３００のネットワークインターフェースＢ２３０３に受信される。ネットワークインターフェースＢ２３０３は受信したパケット２４０１をパケット中継部２３０１に送る。

【０１５５】パケット２４０１を受信したルータ２３００のパケット中継部２３０１の処理を図２５に示されたフローチャートを用いて説明する。

【０１５６】パケット２４０１を受信すると、パケット中継部２３０１は、パケット２４０１の宛先アドレスがルータ２３００のカプセル化用アドレスか判断する（処理２５０１）。パケット２４０１の宛先アドレスは、認証サーバ２３１０のＩＰアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット２４０１の送信元アドレスがＩＰアドレス登録票２３０６に登録されているか検索する（処理２５０２）。送信元アドレスであるユーザ端末２３１２のＩＰアドレスはＩＰアドレス登録表２３０６に登録されていない為、パケット中継部２３０１は、パケット２４０１をカプセル化する（処理２５０３）。そしてパケット中継部２３０１は、カプセル化したパケットを認証サーバ２３１０に送信する（処理２５０４）。

【０１５７】図２６に示されるように、認証サーバ２３１０は、カプセル化されたパケットを受信すると、パケットの宛先アドレスが認証サーバのカプセル化用アドレスか判断する（処理２６０１）。カプセル化されたパケットの宛先アドレスは認証サーバのカプセル化用アドレスである為、パケットの送信元アドレスがルータ２３００のカプセル化用アドレスであるか判断する（処理２６０２）。送信元アドレスはルータのカプセル化用アドレスである為、受信したパケットのカプセル化を解除し、元々のパケット２４０１を取り出す（処理２６０３）。次に、認証サーバ２３１０は、カプセル化を解除したパケット２４０１の宛先アドレスが認証サーバのＩＰアドレスであるか判断する（処理２６０４）。パケット２４０１の宛先アドレスは認証サーバ２３１０のＩＰアドレスである為、認証を行う（処理２６０５）。認証の処理において、認証サーバ２３１０は、パケット２４０１に含まれるユーザＩＤとパスワードがネットワークの使用許可を与えられたユーザのものと一致するか比較し、一致したら、ユーザ端末２３１２の認証が成功したことを通知するパケット２４０２を生成し、更にこのパケット２４０２をカプセル化して送信する（処理２６０６）。パケット２４０２は宛先アドレスとしてユーザ端末２３１２のＩＰアドレスを含むＩＰヘッダを持つ。認証サーバ２３１０によるカプセル化は、宛先アドレスとしてルータ２３００のカプセル化用アドレス（１９２．１６８．１００．１０１）、送信元アドレスとして認証サーバ２３１０のカプセル化用アドレス（１９２．１６８．１００．１００）を含むＩＰヘッダを、パケット２４０２に付加し、新たなパケット（カプセル化したパケット）を作成することである。従って、カプセル化されたパケットはルータ２３００に送信される。

【０１５８】カプセル化されたパケットはネットワークインターフェースＡ２３０２により受信され、パケット中継部２３０１に送られる。図２５に示されたフローチャートに従って、パケット中継部２３０１は、受信した

パケットの宛先アドレスがルータのカプセル化用アドレスか判断する（処理２５０１）。宛先アドレスはルータ２３００のカプセル化用アドレスである為、送信元アドレスが認証サーバ２３１０のカプセル化用アドレスであるか判断する（処理２５０５）。送信元アドレスは認証サーバ２３１０のカプセル化用アドレスである為、パケット中継部２３０１は、受信したパケットのカプセル化を解除し、元々のパケット２４０２を取り出す（処理２５０６）。そして、パケット中継部２３０１は、パケット２４０２を中継し（処理２５０７）、ユーザ端末２３１２へ送信する。

【０１５９】また、ユーザ端末２３１２の認証が成功すると、認証サーバ２３１０は、ルータ２３００に対して、ユーザ端末２３１２のＩＰアドレス（１９２．１６８．３．３）をＩＰアドレス登録表２３０６へ登録するよう指示するパケット２４０３を送信する。

【０１６０】パケット２４０３はネットワークインターフェースＡ２３０２により受信され、パケット中継部２３０１に送られる。パケット中継部２３０１は、パケット２４０３を受け取ると、パケット２４０３による指示に従って、ＩＰアドレス登録表２３０６にユーザ端末２３１２のＩＰアドレス（１９２．１６８．３．３）を登録する。

【０１６１】その後、ユーザ端末２３１２がファイルサーバ２３１１にアクセスする場合について説明する。

【０１６２】ユーザ端末２３１２は、ファイルサーバ２３１１にアクセスするため、ファイルサーバ２３１１のＩＰアドレス（１９２．１６８．１０．２）宛のパケット２４０４を送信する。パケット２４０４は、ルータ２３００のネットワークインターフェースＢ２３０３に受信され、パケット中継部２３０１に送られる。

【０１６３】図２５に示されるように、パケット２４０４を受信すると、パケット中継部２３０１は、パケット２４０４の宛先アドレスがルータ２３００のカプセル化用アドレスか判断する（処理２５０１）。パケット２４０４の宛先アドレスは、ファイルサーバ２３１１のＩＰアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット２４０４の送信元アドレスがＩＰアドレス登録表２３０６に登録されているか検索する（処理２５０２）。送信元アドレスであるユーザ端末２３１２のＩＰアドレスはＩＰアドレス登録表２３０６に登録されている為、ルータ中継部２３０１はパケット２４０４を中継し（処理２５０８）、パケット２４０４をファイルサーバ２３１１へ送信する。

【０１６４】ファイルサーバ２３１１は、パケット２４０４を受信すると、ユーザ端末２３１２によって要求されたデータを含むパケット２４０５を応答パケットとして送信する。パケット２４０５は、ネットワークインターフェースＡ２３０２により受信され、パケット中継部２３０１に送られる。パケット中継部２３０１は、パケット２４０５の宛先アドレスがルータ２３００のカプセル化用アドレスか判断する（処理２５０１）。パケット２４０５の宛先アドレスは、ユーザ端末２３１２のＩＰアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット２４０５の送信元アドレスがＩＰアドレス登録表２３０６に登録されているか検索する（処理２５０２）。送信元アドレスであるファイルサーバ２３１１のアドレス（１９２．１６８．１０．２）はＩＰアドレス登録表２３０６に登録されている。そこで、ルータ中継部２３０１はパケット２４０５を中継し（処理２５０８）、パケット２４０５をユーザ端末２３１２に送信する。このように、ユーザ端末２３１２が認証サーバ２３１０による認証を受けた後は、ユーザ端末２３１２からファイルサーバ２３１１へのアクセスが可能となる。

【０１６５】認証サーバ２３１０は、ユーザ端末２３１２の認証が成功した後、定期的にユーザ端末２３１２に対してＩＣＭＰ（Internet Control Message Protocol）に従ったＩＣＭＰエコーリクエスト２４０６を送信し、ＩＣＭＰエコーリクエスト２４０６に対する応答データであるＩＣＭＰエコーリプライ２４０７がユーザ端末２３１２から返送されてくることを確認する。

【０１６６】ＩＣＭＰエコーリクエスト２４０６を送信してから一定時間以内にユーザ端末２３１２からＩＣＭＰエコーリプライ２４０７が送られてこない場合、認証サーバ２３１０は、ユーザ端末２３１２のＩＰアドレス（１９２．１６８．３．３）をＩＰアドレス登録表から削除するよう指示するパケットをルータ２３００に送信する。そのパケットはネットワークインターフェースＡ２３０２により受信され、パケット中継部２３０１に送られる。パケット中継部２３０１は、そのパケットを受け取ると、パケットによる指示に従って、ＩＰアドレス登録表２３０６からユーザ端末２３１２のＩＰアドレス（１９２．１６８．３．３）を削除する。その結果、ユーザ端末２３１２が再び認証を受けるまでは、ユーザ端末２３１２からファイルサーバ２３１１へのアクセスはできなくなる。

【０１６７】以上のように、ルータ２３００を用いることで、認証を受けていないユーザ端末２３１２からファイルサーバ２３１１へのアクセスが防止され、認証を受けたユーザ端末２３１２からファイルサーバ２３１１へのアクセスが許可されるネットワークシステムを構築することができる。また、認証サーバ２３１０が定期的にユーザ端末２３１１からのＩＣＭＰエコーリプライ２４０７の受信を確認することにより、ユーザ端末２３１１がネットワークから離脱したり、ネットワークの使用を中止した場合、ユーザ端末２３１１のＩＰアドレスをＩＰアドレス登録表２３０６から自動的に削除し、ユーザ端末２３１１によるファイルサーバ２３１１へのアクセスを防止することができる。

【０１６８】図２８は、複数のパケット通信装置Ａ～Ｃ２８０１とルータ２８２０によって複数のネットワークが接続されたネットワークシステムの構成図である。

【０１６９】このネットワークシステムは、例えば、パケット通信装置Ａ～Ｃ２８０１と、各パケット通信装置Ａ～Ｃ２８０１と接続されたルータ２８２０と、それぞれネットワーク（ＩＰサブネット）を介してルータ２８２０に接続されたサーバＡ～Ｃ２８０３、フィルタリング状態管理装置２８０２、ＤＨＣＰサーバ２８０７と、各パケット通信装置Ａ～Ｃ２８０１と接続された１つ以上のネットワーク（ＩＰサブネット）を含む情報コンセントシステム２８３０と、情報コンセントシステム２８３０のうちの任意のネットワークに接続される１台以上のユーザ端末２８０６とを含む。各パケット通信装置Ａ～Ｃ２８０１は、アドレス学習テーブル２８１１と、対象外アドレステーブル２８１２と、認証用アドレステーブル２８１３とを備え、情報コンセントシステム２８３０に接続されたユーザ端末２８０６から送られてくるパケットの中継またはフィルタリング（廃棄）を行なう。各パケット通信装置Ａ～Ｃ２８０１はＯＳＩ参照モデルのデータリンク層でパケットの中継を行うＬＡＮスイッチである。各パケット通信装置Ａ～Ｃ２８０１は、ＤＨＣＰリレーエージェント機能を有し、接続された各ＩＰサブネットに対応するＩＰアドレスを持つものとする。

【０１７０】各サーバＡ～Ｃ２８０３は、それぞれユーザ認証部２８０４と認証状態検出部２８０５を備える。ユーザ認証部２８０４はユーザを識別する為の情報を蓄積するユーザアカウント２８４０を備える。認証状態検出部２８０５はサブネットテーブル２８１４を備える。ユーザ認証部２８０４は各サーバＡ～Ｃ２８０３（パーソナルコンピュータ）により実行されるソフトウェアとして実現されている。ユーザ認証部２８０４としては、ＯＳ(Operating System)の持つログイン機能が用いられるが、その他の認証方法、例えばユーザにパスワードを入力させるWWW(World Wide Web)のページ等が用いられても構わない。また、複数のユーザ認証部２８０４がネットワークシステムに存在する場合、その全てが同じ方式のユーザ認証を行ってもよいし、それぞれが異なる方式のユーザ認証を行ってもよい。認証状態検出部２８０５も、各サーバＡ～Ｃ２８０３により実行されるソフトウェアとして実現されている。ユーザ認証部２８０４により認証（ログイン）が行われた場合、ユーザ認証部２８０４は同じサーバ２８０３において動作する認証状態検出部２８０５に対して、認証（ログイン）に成功したユーザ端末のＩＰアドレスを通知する。

【０１７１】フィルタリング状態管理装置２８０２はサブネットテーブル２８１４を備える。フィルタリング状態管理装置２８０２は、各サーバＡ～Ｃ２８０３の認証状態検出部２８０５およびパケット通信装置２８０１とネットワークを介して通信する。

【０１７２】このネットワークシステムにおいて、ユーザは自由にユーザ端末（ノートパソコン等）を情報コンセントシステム２８３０における１つ以上のネットワーク（ＩＰサブネット１４７．３．１．０から１４７．５．３．０）の何れかに接続することができ、ネットワークシステムを利用することができる。

【０１７３】このネットワークシステムにおいて、通信は全てＩＰプロトコル（ＩＰｖ４）に従って行われる。尚、その他の通信プロトコル（例えばＩＰｖ６）が用いられるネットワークシステムであっても構わない。各ネットワーク（ＩＰサブネット）にはＩＰサブネット番号が割り当てられている。尚、サブネットマスクは全て２４ビット長であるとする。各ネットワークに接続された機器には、そのネットワークに属するＩＰアドレスが割り当てられている。図２８においてＩＰと記されている。各ネットワークは全てＩＥＥＥで規定されているＣＳＭＡ／ＣＤ型の８０２．３ネットワークである。尚、各ネットワークは、その他のネットワークであっても構わない。各ネットワークに接続された各機器のインターフェースには物理アドレス（以下、ＭＡＣアドレスと記載する）が設定されている。以下の説明で必要となるＭＡＣアドレスは、図２８においてＭＡＣと記載されている。

【０１７４】情報コンセントシステム２８３０にユーザ端末２８０６が全く接続されていない初期の状態における各装置の設定について説明する。

【０１７５】ユーザ認証部２８０４には、ネットワークの使用が許可されたユーザのユーザＩＤとパスワードとが登録されている。ユーザ認証部２８０４としてＯＳのユーザ認証（ログイン）機能が用いられるので、ＯＳにおけるユーザアカウント２８４０がこの登録情報に該当する。認証状態検出部２８０５およびフィルタリング状態管理装置２８０２にはサブネットテーブル２８１４が設定されている。

【０１７６】図２９はサブネットテーブル２８１４の構成図である。

【０１７７】サブネットテーブル２８１４の各エントリは、サブネットアドレスフィールド２９０１、サブネットマスクフィールド２９０２、フィルタリング状態管理装置のＩＰアドレスフィールド２９０３、パケット通信装置のＩＰアドレスフィールド２９０４からなる。パケット通信装置のＩＰアドレスフィールド２９０４には、サブネットアドレスフィールド２９０１およびサブネットマスクフィールド２９０２に登録されたサブネットアドレス及びサブネットマスクを論理積したアドレスを持つＩＰサブネットが接続されているパケット通信装置２８０１のＩＰアドレスが登録される。ＩＰアドレスフィールド２９０４に登録されたＩＰアドレスを持つパケット通信装置２８０１に指示を出すフィルタリング状態管理装置２８０２のＩＰアドレスがフィルタリング状態管

理装置のＩＰアドレスフィールド２９０３に登録される。ネットワークシステム内のフィルタリング状態管理装置２８０２は１つだけなので、サブネットテーブル２８１４の全エントリのフィルタリング状態管理装置のＩＰアドレスフィールド２９０３には、同じＩＰアドレスが登録されている。尚、ネットワークシステム内に複数のフィルタリング状態管理装置２８０２を設けて、サブネットテーブル２８１４のエントリごとに異なるＩＰアドレスを登録し、フィルタリング状態管理装置２８０２の処理を分散させることも可能である。認証状態検出部２８０５は、ユーザによるログインを検出すると、ユーザの使用するユーザ端末２８０６のＩＰアドレスが属するＩＰサブネットをサブネットテーブル２８１４で検索し、該当するエントリの内容からユーザのログインを通知すべきフィルタリング状態管理装置２８０２を決定する。同様に、フィルタリング状態管理装置２８０２はサブネットテーブル２８１４の内容からログインしたユーザ端末のＩＰアドレスを通知すべきパケット通信装置２８０１を決定する。

【０１７８】各パケット通信装置Ａ～Ｃ２８０１が備えるアドレス学習テーブル２８１１には、初期状態では１つもエントリが登録されていない。アドレス学習テーブル２８１１の内容については後述する。

【０１７９】図３０は認証用アドレステーブル２８１３の構成図である。

【０１８０】認証用アドレステーブル２８１３には、ユーザ認証部２８０４を備えるサーバ２８０３のＩＰアドレスと、その他にユーザ認証に必要となる機能（例えばＤＮＳ（Domain Name System））を提供する機器のＩＰアドレスが登録される。図３０に示された認証用アドレステーブル２８１３には、各サーバＡ～Ｃ２８０３のＩＰアドレスが登録されている。また、認証用アドレステーブル２８１３は、ユーザ認証を受けていないユーザにも公開してよい情報を持つサーバのＩＰアドレスを登録する為に利用されても良い。

【０１８１】図３１はパケット通信装置Ａ２８０１の対象外アドレステーブル２８１２の構成図である。

【０１８２】対象外アドレステーブル２８１２には、ユーザが認証を受けなくてもアクセスしてよい情報機器のＭＡＣアドレスが登録される。対象外アドレステーブル２８１２に登録されるべき情報機器は、ルータ等のパケット通信装置、プリンタ等の自発的にユーザ認証（ログイン）を行えない機器などである。これらの機器のＭＡＣアドレスが、その機器と同じネットワークに接続されているパケット通信装置２８０１の対象外アドレステーブル２８１２に登録される。図３１に示された対象外アドレステーブル２８１２には、ルータ２８２０の備えるネットワークインターフェースのうち、パケット通信装置Ａ２８０１と接続されているネットワークインターフェースのＭＡＣアドレスが登録されている。

【０１８３】上述した初期状態で、情報コンセントシステム２８３０にユーザ端末２８０６が接続された場合、ユーザ端末２８０６は、ＤＨＣＰサーバ２８０７に対する通信、ルータ２８２０に対するＡＲＰ(Address Resolution Protocol)通信、およびユーザ認証部２８０４との通信だけが許可される。その他の通信はパケット通信装置Ａ２８０１によりフィルタリングされる。フィルタリングとは、許可されていない通信の為のパケットを廃棄することである。

【０１８４】図２８に示されたネットワークシステムにおいて、ユーザによってユーザ端末２８０６が情報コンセントシステム２８３０におけるネットワーク（ＩＰサブネット１４７．３．３．０）に接続され、ユーザ端末２８０６によりユーザ認証（ログイン）が行われる場合の通信シーケンス図を図３３に示す。

【０１８５】ユーザ端末２８０６が認証（ログイン）を行うために通信するサーバ２８０３はサーバＡであるとし、サーバＡのＩＰアドレス１３７．１．１．１はユーザ端末２８０６またはユーザ端末２８０６のユーザに既知であるものとする。

【０１８６】情報コンセントシステム２８３０のネットワーク（ＩＰサブネット１４７．３．３．０）にユーザ端末２８０６が接続された場合、その時点ではユーザ端末２８０６にはＩＰアドレスが割り当てられていない。そこで、図２８に示されたネットワークシステムにおいては、ＤＨＣＰを使ってユーザ端末２８０６にＩＰアドレスが割り当てられる。尚、ＤＨＣＰ以外の方法によってユーザ端末２８０６にＩＰアドレスが割り当てられても構わない。例えば、ユーザ自身によってユーザ端末２８０６にＩＰアドレスが設定されても構わない。ＤＨＣＰ以外の方法が用いられる場合、パケット通信装置２８０１のＤＨＣＰリレーエージェント機能は不要である。

【０１８７】まず、ユーザ端末２８０６が情報コンセントシステム２８３０のネットワーク（ＩＰサブネット１４７．３．３．０）に接続されると、ユーザ端末２８０６は、ＤＨＣＰプロトコルによりＩＰアドレスを要求する為のアドレス要求パケットを送信する。この場合、ユーザ端末２８０６は、パケットの宛先アドレスをブロードキャストアドレスとしてブロードキャスト送信する。アドレス要求パケットはパケット通信装置Ａ２８０１により受信される。

【０１８８】図３２は、パケットを受信した各パケット通信装置Ａ～Ｃ２８０１の中継処理を示すフローチャートである。

【０１８９】パケット通信装置Ａ２８０１は、ユーザ端末２８０６からアドレス要求パケットを受信すると、パケットに含まれる送信元ＭＡＣアドレス（２２：２２：００：１１：１１：１１）をアドレス学習テーブル２８１１から検索する（処理３２０１）。アドレス学習テーブル２８１１には、初期状態ではエントリが登録されて

いない為、パケットの送信元ＭＡＣアドレスを対象外アドレステーブル２８１２から検索する（処理３２０２）。しかし、図３１に示されるように、対象外アドレステーブル２８１２にはルータ２８２０のＭＡＣアドレスしか登録されていない。つまり、ユーザ端末２８０６からのパケットに含まれる送信元ＭＡＣアドレスは何れのテーブルにも登録されていない。よって、パケット通信装置Ａ２８０１は、送信元ＭＡＣアドレスをアドレス学習テーブル２８１１の１つのエントリに登録する。

【０１９０】その後、パケット通信装置Ａ２８０１は、アドレス要求パケットの宛先ＩＰアドレスを認証用アドレステーブル２８１３から検索しようと試みる（処理３２０４）。しかし、アドレス要求パケットの宛先アドレスはブロードキャストアドレスである為、認証用アドレステーブル２８１３には登録されていない。そこで、パケット通信装置Ａ２８０１は、受信したパケットがＤＨＣＰによるアドレス要求パケットであるか判断する（処理３２０５）。受信したパケットはアドレス要求パケットである為、パケット通信装置Ａ２８０１は、ＤＨＣＰリレーエージェント機能により、アドレス要求パケットをルータ２８２０を介してＤＨＣＰサーバ２８０７に中継する（処理３２０８）。

【０１９１】図３３において、ＤＨＣＰサーバ２８０７はアドレス要求パケットを受信し、ユーザ端末２８０６に対してＩＰアドレスを割り当てる。ＤＨＣＰサーバ２８０７は、ユーザ端末２８０６と接続されたネットワーク（ＩＰサブネット１４７．３．３．０）に属するＩＰアドレス（１４７．３．３．１）をユーザ端末２８０６に割り当てる。そして、そのＩＰアドレスをユーザ端末２８０６に通知する為にアドレス配布パケットを送信する。その際、ユーザ端末２８０６が接続されたネットワーク（ＩＰサブネット１４７．３．３．０）におけるデフォルトゲートウェーのアドレスとして、ルータ２８２０のＩＰアドレス１４７．３．３．２５１もアドレス配布パケットに含めてユーザ端末２８０６に通知する。ルータ２８２０のＩＰアドレス１４７．３．３．２５１についてはアドレス配布パケットとは異なるパケットを用いてユーザ端末２８０６に通知しても構わない。なお、デフォルトゲートウェーのアドレスをユーザ端末２８０６に設定する方法として、その他の方法（例えばユーザが入力する）を用いても構わない。アドレス配布パケットはルータ２８２０によりパケット通信装置Ａ２８０１に中継される。パケット通信装置Ａ２８０１は、上述と同様に受信パケットを処理し、ＤＨＣＰリレーエージェント機能により、アドレス配布パケットをユーザ端末のＭＡＣアドレス（２２：２２：００：１１：１１：１１）宛に送る。これにより、ユーザ端末２８０６にＩＰアドレス（１４７．３．３．１）が割り当てられる。

【０１９２】次に、ユーザ端末２８０６がサーバＡ２８０３のユーザ認証部２８０４に対して認証（ログイン）を行う場合について説明する。

【０１９３】ユーザ端末２８０６は、ＩＰアドレスが割り当てられると、サーバＡ２８０３のユーザ認証部に対して認証（ログイン）を試みる。ユーザ端末２８０６とサーバＡは互いに異なるネットワーク（ＩＰサブネット）に属するため、両者はルータ２８２０を経由して通信することになる。

【０１９４】図３３において、ユーザ端末２８０６は、ＤＨＣＰサーバから通知されたデフォルトゲートウェーのＩＰアドレス１４７．３．３．２５１に対応するＭＡＣアドレスを得るために、宛先アドレスとしてブロードキャストアドレスを含むＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１をブロードキャスト送信する。ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１には、送信元ＭＡＣアドレス及び送信元ＩＰアドレスとして、それぞれユーザ端末２８０６のＭＡＣアドレス及びＩＰアドレスが含まれる。

【０１９５】ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１は、パケット通信装置Ａ２８０１により受信される。ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１を受信すると、パケット通信装置Ａ２８０１は、まずＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１に対してＡＲＰパケット学習処理を行い、次にＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１の中継処理を行う。

【０１９６】図３４は、各パケット通信装置Ａ～Ｃ２８０１によるＡＲＰパケット学習処理を示すフローチャートである。

【０１９７】ＡＲＰパケット学習処理において、パケット通信装置Ａ２８０１は、まずＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１に含まれる送信元ＭＡＣアドレスを対象外アドレステーブル２８１２から検索する（処理３４０１）。図３１に示されている通り、対象外アドレステーブル２８１２にはルータ２８２０のＭＡＣアドレスだけが登録されているので、その送信元ＭＡＣアドレスが登録されたエントリは対象外アドレステーブル２８１２にはない。そこで、パケット通信装置Ａ２８０１は、その送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索する（処理３４０２）。初期状態では、パケット通信装置Ａ２８０１の学習テーブル２８１１には何も登録されていない。その為、学習テーブル２８１１にも、その送信元ＭＡＣアドレスが登録されたエントリは無い。次に、パケット通信装置Ａ２８０１は、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１に含まれる送信元ＩＰアドレスをアドレス学習テーブル２８１１から検索する（処理３４０３）。同様に学習テーブル２８１１には何も登録されていない為、その送信元ＩＰアドレスが登録されたエントリは学習テーブル２８１１には無い。よって、パケット通信装置Ａ２８０１はＡＲＰパケット学習処理を終了する。

【０１９８】その後、パケット通信装置Ａ２８０１は図

３２に示されたフローチャートに従って、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１の中継処理を行う。即ち、パケット通信装置Ａ２８０１は、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１に含まれる送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索する（処理３２０１）。上述した通り、アドレス学習テーブル２８１１には何も登録されていないため、パケット通信装置Ａ２８０１は、その送信元ＭＡＣアドレスを対象外アドレステーブル２８１２から検索する（処理３２０２）。図３１に示されるように対象外アドレステーブル２８１２にはルータ２８２０のＭＡＣアドレスだけが登録されており、その送信元ＭＡＣアドレスは何れのエントリにも登録されていない。そこで、パケット通信装置Ａ２８０１は、その送信元ＭＡＣアドレスをアドレス学習テーブル２８１１に登録する（処理３２０３）。

【０１９９】図３５、図３６及び図３７はアドレス学習テーブル２８１１の構成図である。

【０２００】アドレス学習テーブル２８１１の各エントリは、ＭＡＣアドレスフィールド、ＩＰアドレスフィールド、状態フィールド、有効期間フィールドを備える。各エントリのＭＡＣアドレスフィールドには、パケット通信装置２８０１に接続されたユーザ端末２８０６のＭＡＣアドレスが登録される。ＩＰアドレスフィールドには、同じエントリに登録されたＭＡＣアドレスを持つユーザ端末２８０６に割り当てられたＩＰアドレスが登録される。ユーザ端末２８０６のＩＰアドレスが不明または割り当てられていない場合には「０．０．０．０」が登録される。状態フィールドには、同じエントリに登録されたＭＡＣアドレスと一致する送信元ＭＡＣアドレスを含むパケットを廃棄することを示す情報（フィルタリング ＯＮ）、または中継することを示す情報（フィルタリング ＯＦＦ）が登録される。有効期間フィールドには、そのエントリが有効である残り時間（有効時間）が秒単位で保持されている上述した通り、パケット通信装置Ａ２８０１は、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１の送信元アドレスであるユーザ端末２８０６のＭＡＣアドレス（２２：２２：００：１１：１１：１１）をアドレス学習テーブル２８１１のＭＡＣアドレスフィールドに登録し、ＩＰアドレスフィールドに「０．０．０．０」を、状態フィールドに廃棄を示す情報「フィルタリング ＯＮ」を、有効期間フィールドに「３６００秒」を登録する。この状態におけるアドレス学習テーブルの構成図を図３５に示す。

【０２０１】「３６００秒」という時間は、ネットワークに接続されたユーザ端末２８０６が、ＩＰアドレスの割り当ても受けず認証（ログイン）も行わなかった場合に、アドレス学習テーブル２８１１からエントリが削除されるまでの時間に相当する。尚、ＩＰアドレスの割り当てや、認証（ログイン）処理にかかる時間より大きい時間であれば、エントリの有効期間「３６００秒」とは異なる任意の時間でもよい。また、エントリの有効期間が、パケット通信装置２８０１と同じネットワークに接続された装置に備えられるＡＲＰキャッシュ内の情報の有効期間より短い期間であると、パケット通信装置２８０１とその装置とで情報の不一致が起こる可能性がある。そのため、エントリの有効期間は、ＡＲＰキャッシュ内の情報の有効期間より長い時間とする。

【０２０２】次に、パケット通信装置Ａ２８０１は、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１に含まれる宛先ＩＰアドレスを認証用アドレステーブル２８１３から検索する（処理３２０４）。しかし、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１はＩＰパケットではない為、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１がＤＨＣＰパケットであるか判断する（処理３２０５）。ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１がＤＨＣＰパケットではない為、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１に含まれる宛先ＭＡＣアドレスがブロードキャストアドレスか判断する（処理３２０６）。宛先ＭＡＣアドレスはブロードキャストアドレスである為、パケット通信装置Ａ２８０１は、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１をルータ２８２０にのみ中継する（処理３２０９）。

【０２０３】ルータ２８２０は、ＡＲＰ Ｒｅｑｕｅｓｔパケット３３０１を受信し、ＡＲＰ Ｒｅｐｌｙパケット３３０２を送信する。ＡＲＰ Ｒｅｐｌｙパケット３３０２は、送信元ＭＡＣアドレス及び送信元ＩＰアドレスとして、それぞれルータ２８２０のＭＡＣアドレス（２２：２２：００：００：００：０３）及びＩＰアドレス（１４７．３．３．２５１）を含む。

【０２０４】パケット通信装置Ａ２８０１はＡＲＰ Ｒｅｐｌｙパケット３３０２を受信し、ＡＲＰパケット学習処理と中継処理を以下のように行う。

【０２０５】ＡＲＰパケット学習処理において、パケット通信装置Ａ２８０１は、まずＡＲＰ Ｒｅｐｌｙパケット３３０２に含まれる送信元ＭＡＣアドレスを対象外アドレステーブル２８１２から検索する（処理３４０１）。図３１に示されている通り、対象外アドレステーブル２８１２には、ルータ２８２０のＭＡＣアドレスが登録されている。従って、パケット通信装置Ａ２８０１は、送信元ＭＡＣアドレスであるルータ２８２０のＭＡＣアドレスが登録されたエントリを対象外アドレステーブル２８１２から見つけ、ＡＲＰパケット学習処理を終了する。

【０２０６】次に、パケット通信装置Ａ２８０１は、図３２に示されたフローチャートに従って、ＡＲＰ Ｒｅｐｌｙパケット３３０２に含まれる送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索する（処理３２０１）。アドレス学習テーブル２８１１にはルータ２８２０のＭＡＣアドレスは登録されていないため、パケット通信装置Ａ２８０１は、その送信元ＭＡＣアドレスを対象外アドレステーブル２８１２から検索する（処

理３２０２）。対象外アドレステーブル２８１２には送信元ＭＡＣアドレスであるルータ２８２０のＭＡＣアドレスが登録されている為、パケット通信装置Ａ２８０１はＡＲＰ　Ｒｅｐｌｙパケット３３０２を中継し（処理３２１１）、ユーザ端末２８０６に送信する。ユーザ端末２８０６は、ＡＲＰ　Ｒｅｐｌｙパケット３３０２を受信し、ルータ２８２０のＭＡＣアドレスを認識する。

【０２０７】ユーザ端末２８０６は、認証（ログイン）を行うため、サーバＡ２８０３のユーザ認証部２８０４に対してログイン要求パケット３３０３を送信する。ログイン要求パケット３３０３は、宛先ＩＰアドレスとしてサーバＡ２８０３のＩＰアドレス、宛先ＭＡＣアドレスとしてルータ２８２０のＭＡＣアドレス、送信元ＭＡＣアドレス及び送信元ＩＰアドレスとして、それぞれユーザ端末２８０６のＭＡＣアドレス及びＩＰアドレスを含む。パケット通信装置Ａ２８０１はログイン要求パケット３３０３を受信し、図３２に示されたフローチャートに従って、ログイン要求パケット３３０３に含まれる送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索する（処理３２０１）。アドレス学習テーブル２８１１にはユーザ端末２８０６のＭＡＣアドレスが既に登録されている。そこで、パケット通信装置Ａ２８０１は、送信元ＭＡＣアドレスが登録されているエントリの状態フィールドを参照する。図３５に示される通り、状態フィールドは「フィルタリング　ＯＮ」を示している為、ログイン要求パケット３３０３に含まれる宛先ＩＰアドレスを認証用アドレステーブル２８１３から検索する（処理３２０４）。認証用アドレステーブル２８１３にはサーバＡ２８０３のＩＰアドレスが登録されている為、パケット通信装置Ａ２８０１はログイン要求パケット３３０３に含まれる送信元ＩＰアドレスがアドレス学習テーブル２８１１に登録されているか参照する。図３５に示される通り、アドレス学習テーブル２８１１のユーザ端末２８０６のＭＡＣアドレスが登録されたエントリにおけるＩＰアドレスフィールドには「０．０．０．０」が登録されており、ユーザ端末２８０６のＩＰアドレスは登録されていない。従って、パケット通信装置Ａ２８０１は、そのＩＰアドレスフィールドに、送信元ＩＰアドレスであるユーザ端末２８０６のＩＰアドレス（１４７．３．３．１）を登録する（処理３２１０）。この場合、パケット通信装置Ａ２８０１は有効期間フィールドに保持された時間値は変更しない。

【０２０８】この状態におけるアドレス学習テーブルの構成図を図３６に示す。

【０２０９】そして、パケット通信装置Ａ２８０１はログイン要求パケット３３０３を中継し（処理３２１１）、ルータ２８２０に送る。ログイン要求パケット３３０３はルータ２８２０によりサーバＡ２８０３へ中継される。

【０２１０】サーバＡ２８０３がログイン要求パケット３３０３を受信すると、サーバＡ２８０３のユーザ認証部２８０４は、ユーザ端末２８０６に対してパスワードの入力を要求するパスワード要求パケット３３０４を送信する。ルータ２８２０はパスワード要求パケット３３０４を中継し、パケット通信装置Ａ２８０１に送る。この際、ルータ２８２０は、パスワード要求パケット３３０４に含まれる送信元ＭＡＣアドレスをルータ２８２０のＭＡＣアドレスにして送信する。パケット通信装置Ａ２８０１は、パスワード要求パケット３３０４を受信する。パケット通信装置Ａ２８０１は、図３２に示されたフローチャートに従って、ＡＲＰ　Ｒｅｐｌｙパケット３３０２の中継処理と同様にして、パスワード要求パケット３３０４に含まれる送信元アドレスをアドレス学習テーブル２８１１及び対象外アドレステーブル２８１２から検索する（処理３２０１及び処理３２０２）。対象外アドレステーブル２８１２には送信元ＭＡＣアドレスであるルータ２８２０のＭＡＣアドレスが登録されている為、パケット通信装置Ａ２８０１はパスワード要求パケット３３０４を中継し（処理３２１１）、ユーザ端末２８０６に送信する。ユーザ端末２８０６がパスワード要求パケット３３０４を受信すると、ユーザ端末２８０６においてユーザに対してパスワードの入力が促される。ユーザは、ユーザ端末２８０６にパスワードを入力する。ユーザ端末２８０６は、入力されたパスワードを含むパケット３３０５を送信する。パケット通信装置Ａ２８０１は、パケット３３０５を受信し、ログイン要求パケット３３０３の中継処理と同様にして、パケット３３０５に含まれる送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索し（処理３２０１）、また、パケット３３０５に含まれる宛先ＩＰアドレスを認証用アドレステーブル２８１３から検索する（処理３２０４）。認証用アドレステーブル２８１３には宛先ＩＰアドレスであるサーバＡ２８０３のＩＰアドレスが登録されており、また、送信元ＩＰアドレスであるユーザ端末２８０６のＩＰアドレスもアドレス学習テーブル２８１１に登録されている為（処理３２１０）、パケット通信装置Ａ２８０１はパケット３３０５中継し、ルータ２８２０に送信する。パケット３３０５はルータ２８２０によりサーバＡ２８０３へ中継される。サーバＡ２８０３がパケット３３０５を受信すると、ユーザ認証部２８０４はパケット３３０５に含まれるパスワードと、ユーザアカウント２８４０ととして保持している正規のパスワードとを比較し、パスワードが正しいか判定する。ユーザ認証部２８０４によりパケット３３０５に含まれるパスワードが正しいと判定されると、ユーザ端末２８０６のログインがユーザ認証部２８０４により許可される。ユーザ認証部２８０４は、ユーザ端末２８０６に対してログイン完了を通知するログイン完了パケット３３０６を送信し、また、サーバＡ２８０３内の認証状態検出部２８０５に対してユーザ端末２８０６のＩＰアドレス

（１４７．３．３．１）とログインの完了を知らせる。

【０２１１】認証状態検出部２８０５は、サブネットテーブル２８１４の各エントリのうち、サブネットマスクフィールド２９０２に保持されたサブネットマスクとユーザ端末２８０６のＩＰアドレスを論理積したアドレスが、サブネットアドレスフィールド２９０１に保持されたサブネットアドレスと一致するようなエントリを検索する。認証状態検出部２８０５は、該当するエントリを見つけると、そのエントリのフィルタリング状態管理装置のＩＰアドレスフィールド２９０３に登録されたＩＰアドレス宛に、ユーザ端末２８０６のＩＰアドレスを含む接続通知パケット３３０７を送信する。例えば、図２９に示されたサブネットテーブルにおいて、＃３のエントリが、ユーザ端末２８０６と接続されたネットワーク（ＩＰサブネット）のサブネットアドレスを含み、上述のエントリに該当する。従って、＃３のエントリから、接続通知パケット３３０７を送るべきフィルタリング状態管理装置２８０２のＩＰアドレスは「１３７．２．２．１００」であることがわかる。

【０２１２】接続通知パケット３３０７はルータ２８２０によりフィルタリング状態管理装置２８０２に中継される。フィルタリング状態管理装置２８０２は、接続通知パケット３３０７を受け取ると、サブネットテーブル２８１４のエントリのうち、サブネットマスクフィールド２９０２に保持されたサブネットマスクと、通知されたユーザ端末２８０６のＩＰアドレスを論理積したアドレスが、サブネットアドレスフィールド２９０１に保持されたサブネットアドレスと一致するようなエントリを検索する。該当するエントリを見つけると、そのエントリのパケット通信装置のＩＰアドレスフィールド２９０４に保持されたＩＰアドレスを認識する。図２９に示されたサブネットテーブルにおいては＃３のエントリが上述したエントリに該当する為、＃３のエントリから、パケット通信装置のＩＰアドレスは「１４７．３．１．２２０」（パケット通信装置Ａ２８０１のＩＰアドレス）であることがわかる。フィルタリング状態管理装置２８０２は、認識したＩＰアドレスを持つパケット通信装置Ａ２８０１宛に、ユーザ端末２８０６のＩＰアドレス（１４７．３．３．１）を含む接続許可パケット３３０８を送信する。

【０２１３】接続許可パケット３３０８を通知されたパケット通信装置Ａ２８０１は、通知されたユーザ端末２８０６のＩＰアドレス（１４７．３．３．１）をアドレス学習テーブル２８１１から検索する。図３６に示される通り、ユーザ端末２８０６のＩＰアドレスはアドレス学習テーブル２８１１の１つのエントリに登録されている。その為、パケット通信装置Ａ２８０６は、そのエントリの状態フィールドに登録されている情報を「フィルタリング　ＯＮ」から「フィルタリング　ＯＦＦ」へ変更し、また、有効期間フィールドに新たに「３００秒」という時間を設定する。

【０２１４】この状態におけるアドレス学習テーブルの構成図を図３７に示す。

【０２１５】その後、送信元ＭＡＣアドレスとしてユーザ端末２８０６のＭＡＣアドレス（２２：２２：００：１１：１１：１１）を含むパケットを受信すると、パケット通信装置２８０１は、図３２に示されたフローチャートに従って、送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索する（処理３２０１）。この場合、アドレス学習テーブル２８１１のエントリの１つに送信元ＭＡＣアドレスが登録されており、また、そのエントリの状態フィールドは「フィルタリングＯＦＦ」を示している。その為、パケット通信装置Ａ２８０１は常に受信したパケットを中継する（処理３２１１）。その結果、ユーザ端末２８０６から送信されるパケットはパケット通信装置２８０１によって廃棄されることがない為、ユーザ端末２８０１は自由に通信を行うことができる。

【０２１６】次に、ユーザ端末２８０６がネットワークから離脱した場合のパケット通信装置Ａ２８０１における検出方法と処理について説明する。

【０２１７】パケット通信装置Ａ２８０１は、アドレス学習テーブル２８１１の各エントリにおける有効期間フィールドの更新処理を一定時間ごとに起動する。例えば、パケット通信装置Ａ２８０１は３０秒毎に有効期間フィールドの更新処理を起動する。起動する周期は、エントリの有効期間をどの程度の精度で保証するかに依存する。

【０２１８】このアドレス学習テーブルにおける有効期間フィールドの更新処理について図３８を用いて説明する。

【０２１９】図３８は、各パケット通信装置Ａ～Ｃ２８０１によるアドレス学習テーブル２８１１の更新処理を示すフローチャートである。

【０２２０】パケット通信装置Ａ２８０１において、アドレス学習テーブル２８１１の更新処理が起動されると、まず、アドレス学習テーブル２８１１の各エントリにおける有効期間フィールドに保持されている残り時間（有効時間）から、更新処理の起動間隔である「３０秒」が減算され、有効時間が更新される（処理３８０１）。減算された結果、有効期間フィールドに保持されている残り時間（更新された有効時間）が６０秒（起動間隔の２倍）より大きい値である場合、パケット通信装置Ａ２８０１はそのエントリに関してそれ以上の処理を行わず、一旦更新処理を終了する。更新された有効時間が０秒より大きく６０秒以下の値であるエントリが存在する場合、パケット通信装置Ａ２８０１は、そのエントリに登録されているＩＰアドレスを割り当てられているユーザ端末２８０６のＭＡＣアドレスを再確認する為に、ＡＲＰ　Ｒｅｑｕｅｓｔパケットを、そのユーザ端

末２８０６が接続されているＩＰサブネットに送信する（処理３８０３）。更新された有効時間が０秒以下であるエントリが存在する場合、パケット通信装置Ａ２８０１はそのエントリを削除する（処理３８０４）。これによって、アドレス学習テーブル２８１１は、そのエントリに登録されていたＭＡＣアドレスを持つユーザ端末２８０６がネットワークに接続される前の状態に戻る。

【０２２１】以上の更新処理を実行することにより、パケット通信装置Ａ２８０１は、定期的（上述した更新処理においては約４分毎）にＡＲＰ　Ｒｅｑｕｅｓｔパケットを送信し、ユーザ端末２８０６の存在を確認する。ユーザ端末２８０６がネットワークに接続されていれば、ＡＲＰ　Ｒｅｑｕｅｓｔパケットに応じてＡＲＰＲｅｐｌｙパケットがユーザ端末２８０６から送信される。従って、ＡＲＰ　Ｒｅｑｕｅｓｔパケットに対する応答がなければパケット通信装置Ａ２８０１は、ユーザ端末２８０６がネットワークから離脱したと解釈し、更新された有効時間が０秒以下になった時点でそのエントリを削除する。

【０２２２】パケット通信装置Ａ２８０１における更新処理の起動間隔が３０秒であり、パケット通信装置Ａ２８０１がＡＲＰ　Ｒｅｑｕｅｓｔパケットを送信する条件は更新した有効時間が６０秒以下（起動間隔の２倍）となることであるから、１つのエントリが削除されるまでに２回、ＡＲＰ　Ｒｅｑｕｅｓｔパケットが送信されることになる。ＡＲＰ　Ｒｅｑｕｅｓｔパケットが送信される条件を種々設定することにより、パケット通信装置Ａ２８０１がエントリを削除するまでにユーザ端末２８０６の存在を確認する回数を調整することが可能である。

【０２２３】更に、パケット通信装置Ａ２８０１は、ユーザ端末２８０６から送られてくるＡＲＰ　ＲｅｑｕｅｓｔパケットやＡＲＰ　Ｒｅｐｌｙパケットによってアドレス学習テーブル２８１１の有効期間フィールドに保持された有効時間を更新する。パケット通信装置Ａ２８０１が、ユーザ端末２８０６から送られてくるＡＲＰＲｅｑｕｅｓｔパケットまたはＡＲＰ　Ｒｅｐｌｙパケットにより、アドレス学習テーブル２８１１の有効期間フィールドの有効時間を更新する場合の処理を、図３４を用いて説明する。

【０２２４】まず、ユーザ端末２８０６によって認証（ログイン）が行なわれたことにより、アドレス学習テーブル２８１１の１つのエントリには、図３７に示されるようにユーザ端末２８０６のＭＡＣアドレス、ＩＰアドレス、中継を示す情報、及び有効時間が登録されているとし、また、そのエントリに有効時間（３００秒）が登録されてから１２０秒が経過しているとする。従って、アドレス学習テーブル２８１１のそのエントリの有効時間は１８０秒になっている。

【０２２５】パケット通信装置Ａ２８０１は、ユーザ端末２８０６から送られたＡＲＰ　Ｒｅｑｕｅｓｔパケットまたは ＡＲＰ　Ｒｅｐｌｙパケットを受信すると、図３４に示されたフローチャートに従ってＡＲＰパケット学習処理を実行する。まず、ＡＲＰ　ＲｅｑｕｅｓｔパケットまたはＡＲＰ　Ｒｅｐｌｙパケットに含まれる送信元ＭＡＣアドレスを対象外アドレステーブル２８１２から検索する（処理３４０１）。図３１に示されている通り、対象外アドレステーブル２８１２にはユーザ端末２８０６のＭＡＣアドレスは登録されていない。そこで、パケット通信装置Ａ２８０１は、その送信元ＭＡＣアドレスをアドレス学習テーブル２８１１から検索する（処理３４０２）。送信元ＭＡＣアドレスはユーザ端末２８０６のＭＡＣアドレスであり、そのＭＡＣアドレスが登録されたエントリがアドレス学習テーブル２８１１に存在する。よって、パケット通信装置Ａ２８０１は、ＡＲＰ　Ｒｅｑｕｅｓｔパケットまたは ＡＲＰ　Ｒｅｐｌｙパケットに含まれる送信元ＩＰアドレスとアドレス学習テーブル２８１１のそのエントリに登録されたＩＰアドレス（１４７．３．３．１）とを比較する（処理３４０５）。通常、通信中のユーザ端末２８０６に割り当てられたＩＰアドレスは変更される必要はない為、アドレス学習テーブル２８１１に登録されているＩＰアドレスと送信元ＩＰアドレスは一致する。その結果、パケット通信装置Ａ２８０１は、そのエントリに保持されている有効時間が３００秒未満であれば有効時間を３００秒に更新し（処理３４０６）、ＡＲＰパケット学習処理を終了する。この場合、有効時間は１８０秒である為、その有効時間は３００秒に更新される。

【０２２６】ユーザ端末２８０６から送られるＡＲＰ　Ｒｅｑｕｅｓｔパケットまたは ＡＲＰ　Ｒｅｐｌｙパケットを、パケット通信装置Ａ２８０１がアドレス学習テーブル２８１１のエントリの有効時間の更新に利用することにより、実際にパケット通信装置Ａ２８０１がＡＲＰ　Ｒｅｑｕｅｓｔパケットをユーザ端末２８０６に送信する間隔は、上述した定期的な間隔（約４分）よりも長くなる。その為、ユーザ端末２８０６が接続されたネットワークに対する負荷が軽減される。ユーザ端末２８０６が通信している状態では、定期的に、または不定期にユーザ端末２８０６からＡＲＰ　Ｒｅｑｕｅｓｔパケットまたは ＡＲＰ　Ｒｅｐｌｙパケットが送られてくる。その為、パケット通信装置Ａ２８０１によるユーザ端末２８０６へのＡＲＰ　Ｒｅｑｕｅｓｔパケットの送信は、ユーザ端末２８０６が通信を行わずに一定時間が経過した後、つまりユーザ端末２８０６がネットワークから離脱している可能性が高い状態においてのみ、ということになる。

【０２２７】以上の通り、ユーザが自由にユーザ端末を接続できる情報コンセントシステムを備えるネットワークシステムにおいて、パケット通信装置２８０１が用いられることにより、認証（ログイン）を行っていないユ

ーザ端末２８０６のパケットは廃棄され、不正ユーザによるネットワークの利用が防止される。

【０２２８】

【発明の効果】本発明によれば、ユーザが任意の時刻及び任意の場所において情報コンセントにユーザ端末を接続しても、認証を受けたユーザのみがネットワークシステムにおけるファイルサーバ等の資源を利用でき、認証を受けていない不正なユーザによるネットワークシステムの資源の利用が防止される。

【図面の簡単な説明】

【図１】一実施の形態におけるパケット通信装置の構成図。

【図２】ネットワークインターフェース１０２～１０７の構成図。

【図３】アドレス学習テーブル１０８の構成図。

【図４】ＬＡＮ１００が用いられたネットワークシステムの構成図。

【図５】ユーザ端末４０３が情報コンセント４０９に接続された場合の通信シーケンス図。

【図６】ＬＡＮスイッチ１００の中継処理を示すフローチャート。

【図７】アドレス学習テーブル１０８の構成図。

【図８】図６に示された処理６０４のフローチャート。

【図９】中継テーブル９０１の構成図。

【図１０】パケット通信装置の他の構成図。

【図１１】フィルタリング処理部１０１２～１０１７の構成図。

【図１２】フィルタリングテーブル１１０１の構成図。

【図１３】ルータ１０００が用いられたネットワークシステムの構成図。

【図１４】ユーザ端末１３３３が情報コンセント４０９に接続された場合の通信シーケンス図。

【図１５】フィルタリングテーブル１１０１の構成図。

【図１６】パケット通信装置の他の構成図。

【図１７】フィルタリングテーブル１６０７の構成図。

【図１８】学習テーブル１６０６の構成図。

【図１９】ＬＡＮスイッチ１６００が用いられたネットワークシステムの構成図。

【図２０】ユーザ端末１９０５がネットワークＢの情報コンセント４０９に接続された場合の通信シーケンス図。

【図２１】ＬＡＮスイッチ１６００の中継処理を示すフローチャート。

【図２２】学習テーブル１６０６の構成図。

【図２３】ルータ２３００が用いられたネットワークシステムの構成図。

【図２４】ユーザ端末２３１２がネットワークＢ２３１３に接続された情報コンセントに接続された場合の通信シーケンス図。

【図２５】ルータ２３００の中継処理を示すフローチャート。

【図２６】パケットを受信した認証サーバ２３１０の処理を示すフローチャート。

【図２７】初期状態でのＩＰアドレス登録表２３０６の構成図。

【図２８】複数のパケット通信装置Ａ～Ｃ２８０１とルータ２８２０によって複数のネットワークが接続されたネットワークシステムの構成図。

【図２９】サブネットテーブル２８１４の構成図。

【図３０】認証用アドレステーブル２８１３の構成図。

【図３１】対象外アドレステーブル２８１２の構成図。

【図３２】パケット通信装置２８０１の中継処理を示すフローチャート。

【図３３】ユーザ端末２８０６が情報コンセントシステム２８３０におけるネットワークに接続された場合の通信シーケンス図。

【図３４】パケット通信装置２８０１によるＡＲＰパケット学習処理を示すフローチャート。

【図３５】アドレス学習テーブル２８１１の構成図。

【図３６】アドレス学習テーブル２８１１の構成図。

【図３７】アドレス学習テーブル２８１１の構成図。

【図３８】パケット通信装置２８０１によるアドレス学習テーブル２８１１の更新処理を示すフローチャート。

【符号の説明】

１００　ＬＡＮスイッチ
１０９　状態変更指示パケット処理部
２０３　状態管理部
４０１　認証サーバ
４０２　ファイルサーバ
４０３　ユーザ端末
４０９　情報コンセント

【図３０】

図30

2813 認証用アドレステーブル

#	サーバアドレス
1	137.1.1.1
2	137.1.1.2
3	137.1.1.3

【図３１】

図31

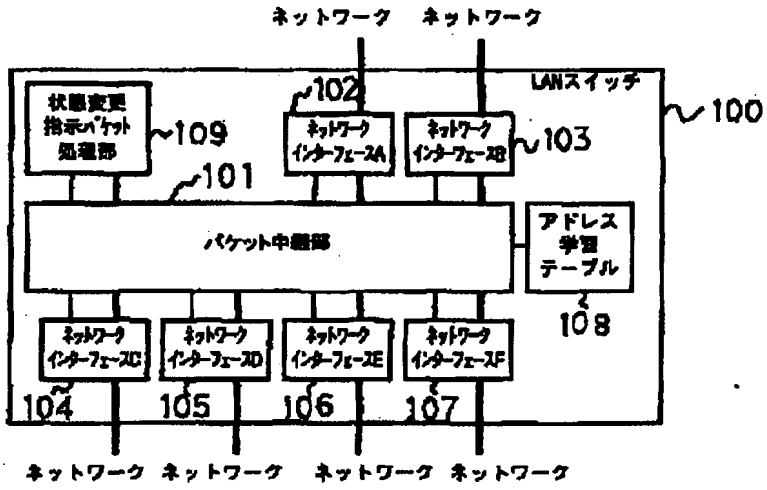
対象外アドレステーブル
(パケット通信装置A)

2812

#	対象外アドレス
1	22:22:00:00:00:09

【図１】

図１



【図７】

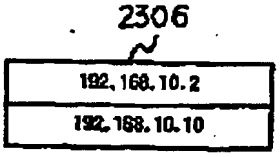
図７

108 301 302

#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:33:33:33	B
3	22:22:00:FF:FF:FF	X
4	22:33:FF:00:00:01	C

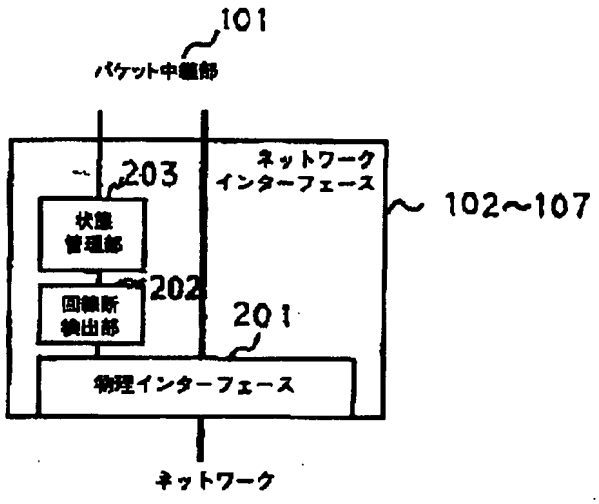
【図２７】

図２７



【図２】

図２



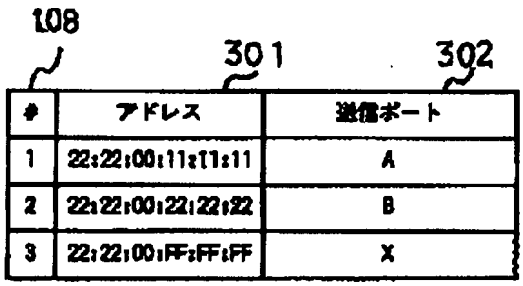
【図２２】

図２２

1606	1801	1802
#	MAC アドレス	接続ポート
1	22:22:00:44:44:44	A
2	22:22:FF:00:00:01	B

【図３】

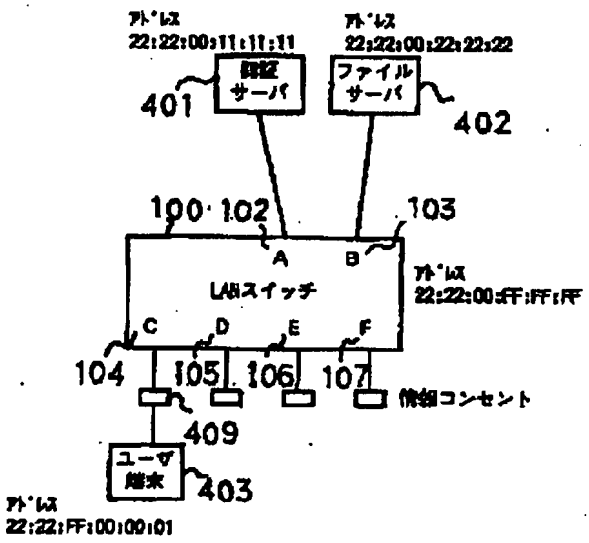
図３



#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X

【図４】

図4



【図１８】

図18

1606	1801	1802
#	MAC アドレス	接続ポート
1	22:22:00:44:44:44	A

【図２９】

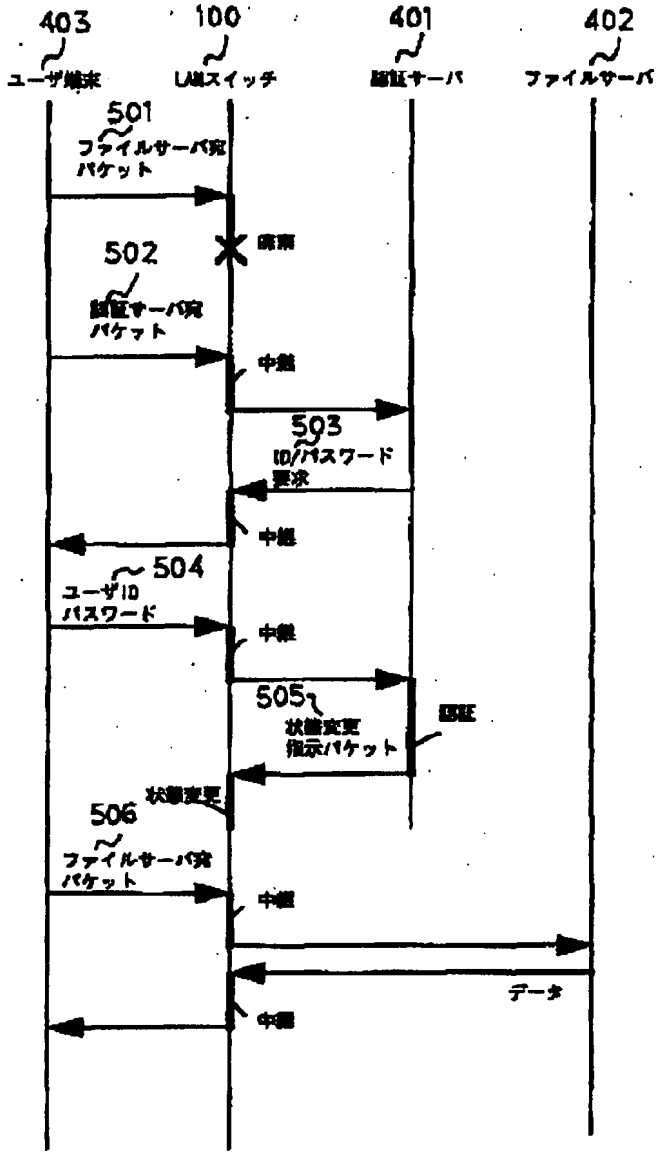
図29

サブネットテーブル

2814	2901	2902	2903	2904
#	サブネットアドレス	サブネットマスク	フィルタリング状態管理装置のIPアドレス	パケット通信装置のIPアドレス
1	147.3.1.0	255.255.255.0	137.2.2.100	147.3.1.220
2	147.3.2.0	255.255.255.0	137.2.2.100	147.3.1.220
3	147.3.3.0	255.255.255.0	137.2.2.100	147.3.1.220
4	147.4.1.0	255.255.255.0	137.2.2.100	147.4.1.220
5	147.4.2.0	255.255.255.0	137.2.2.100	147.4.1.220
6	147.5.1.0	255.255.255.0	137.2.2.100	147.5.1.220
7	147.5.2.0	255.255.255.0	137.2.2.100	147.5.1.220
8	147.5.3.0	255.255.255.0	137.2.2.100	147.5.1.220

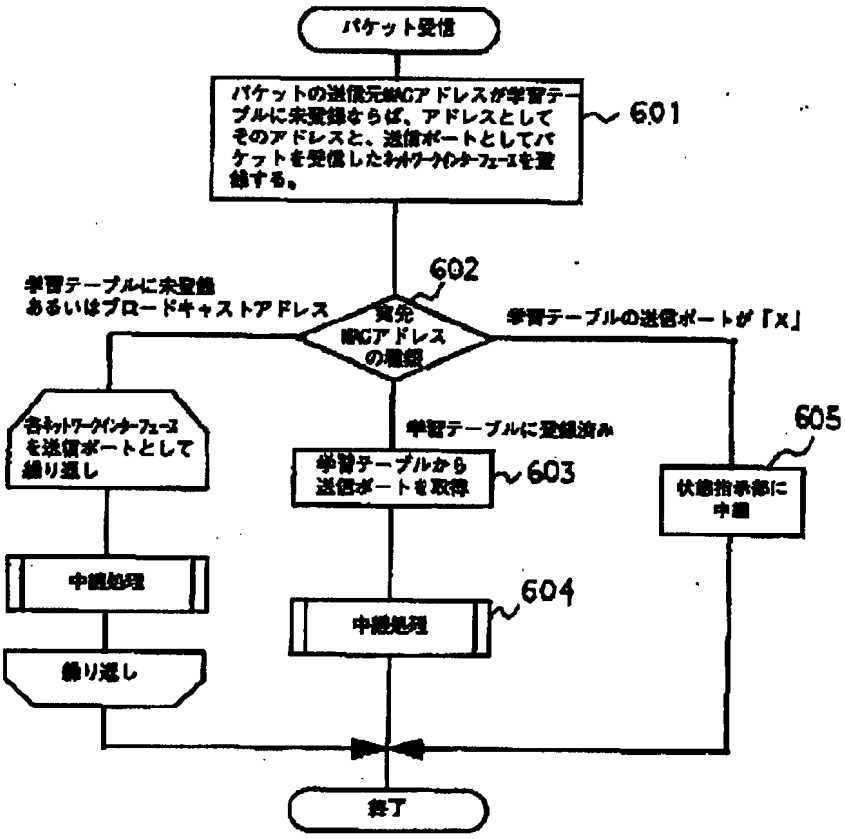
【図５】

図５


403
ユーザ端末
100
LANスイッチ
401
認証サーバ
402
ファイルサーバ
501
ファイルサーバ宛
パケット
破棄
502
認証サーバ宛
パケット
中継
503
ID/パスワード
要求
中継
504
ユーザID
パスワード
中継
505
状態変更
指示パケット
認証
状態変更
506
ファイルサーバ宛
パケット
中継
データ
中継

【図６】

図６



【図３５】

図35

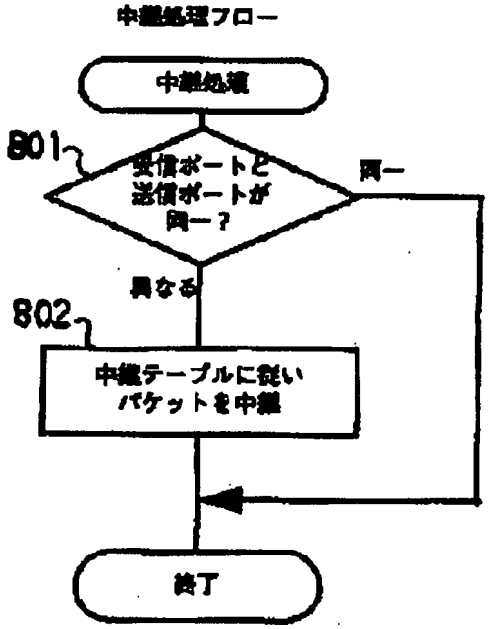
アドレス学習テーブル

2811

#	MACアドレス	IPアドレス	状態	有効期間
1	22:22:00:11:11:11	0.0.0.0	フィルタリング ON	3600秒

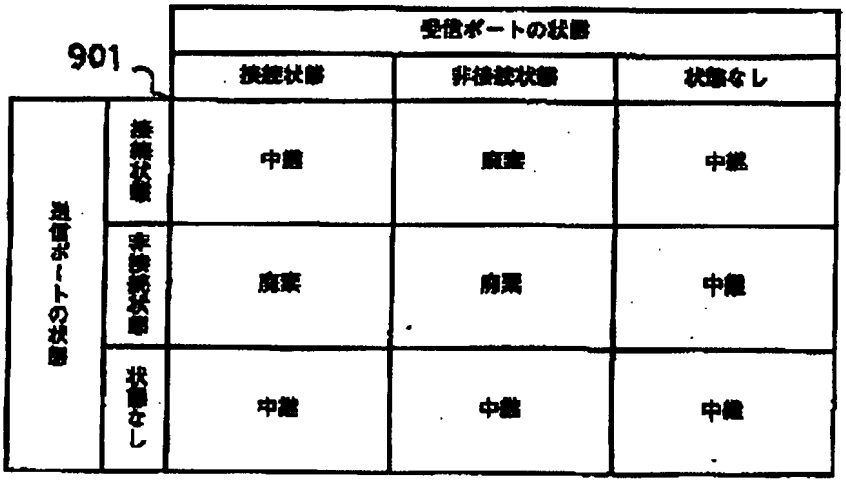
【図８】

図８


中継処理フロー
中継処理
801
受信ポートと
送信ポートが
同一？
同一
異なる
802
中継テーブルに従い
パケットを中継
終了

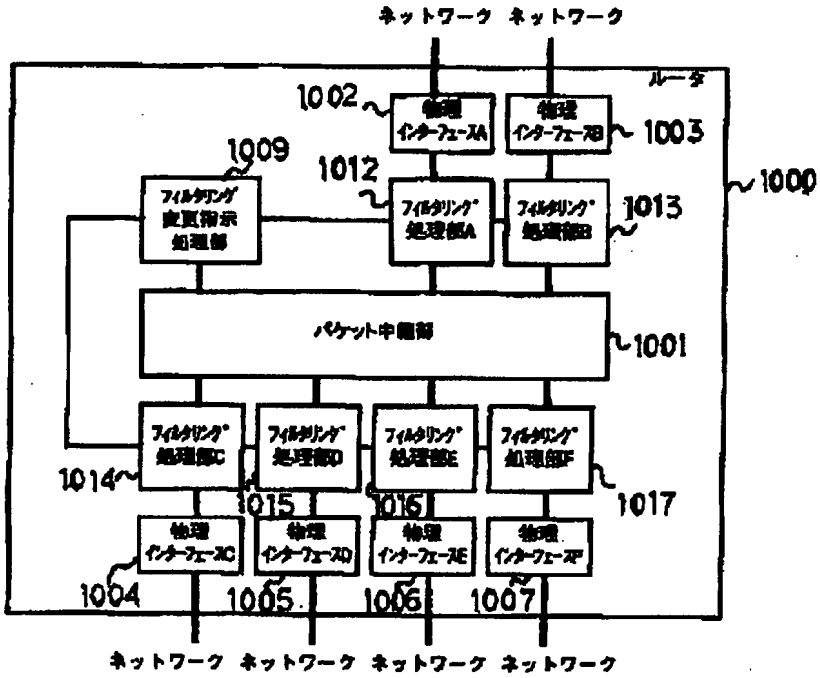
【図９】

図９


901
受信ポートの状態
接続状態
非接続状態
状態なし
送信ポートの状態
接続状態
非接続状態
状態なし
中継
廃棄
中継
廃棄
廃棄
中継
中継
中継
中継

【図１０】

図１０



【図３６】

図36

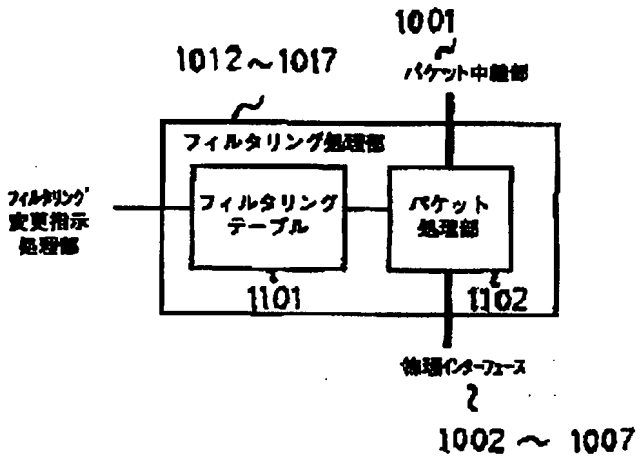
アドレス学習テーブル

2611

#	MACアドレス	IPアドレス	状態	有効期間
1	22:22:00:11:11:11	147.3.3.1	フィルタリング ON	3600秒

【図１１】

図１１



【図３７】

図37

アドレス学習テーブル

2811

#	MACアドレス	IPアドレス	状態	有効期間
1	22:22:00:11:11:11	147.3.3.1	フィルタリング OFF	300秒

【図１２】

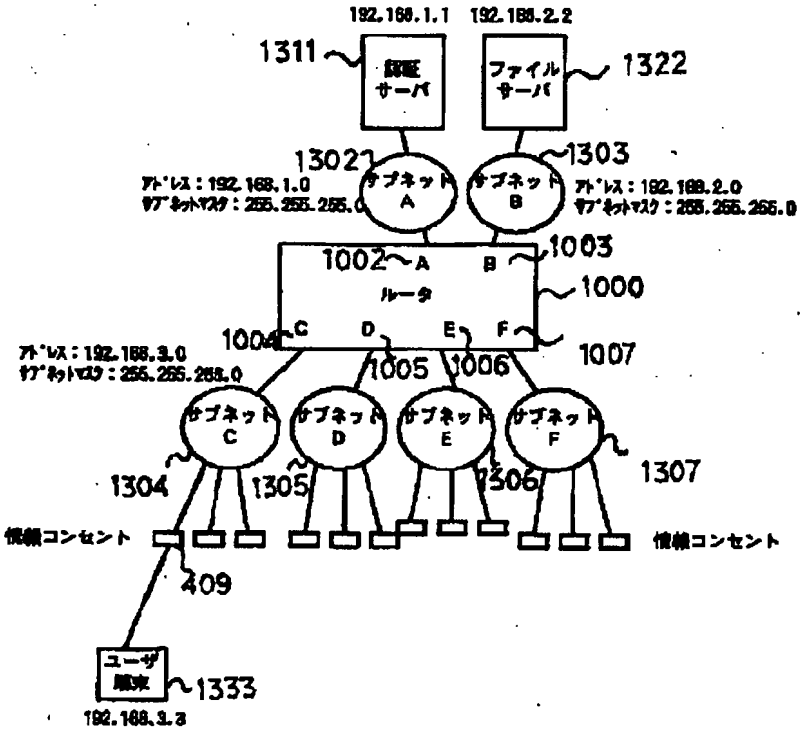
図１２

1101

#	1201 宛先アドレス条件	1202 送信元アドレス条件	1203 中継／廃棄フラグ
1	192.168.1.1	任意	中継
2	任意	任意	廃棄

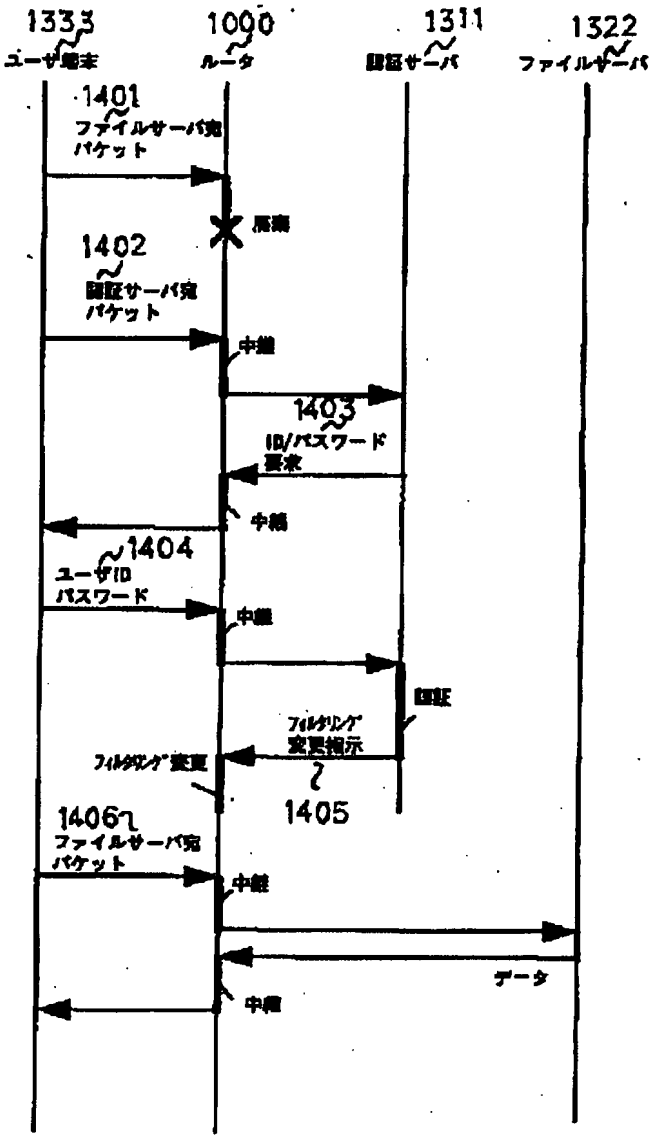
【図１３】

図１３


192.168.1.1
192.168.2.2
1311
認証サーバ
ファイルサーバ
1322
1302
1303
サブネットA
サブネットB
アドレス：192.168.1.0
サブネットマスク：255.255.255.0
アドレス：192.168.2.0
サブネットマスク：255.255.255.0
1002
A
B
1003
ルータ
1000
C
D
E
F
1004
1005
1006
1007
アドレス：192.168.3.0
サブネットマスク：255.255.255.0
サブネットC
サブネットD
サブネットE
サブネットF
1304
1305
1306
1307
情報コンセント
情報コンセント
409
ユーザ端末
1333
192.168.3.3

【図１４】

図１４


1333
ユーザ端末
1090
ルータ
1311
認証サーバ
1322
ファイルサーバ
1401
ファイルサーバ宛
パケット
障害
1402
認証サーバ宛
パケット
中継
1403
ID/パスワード
要求
中継
1404
ユーザID
パスワード
中継
認証
フィルタリング
変更指示
フィルタリング変更
1405
1406
ファイルサーバ宛
パケット
中継
データ
中継

【図１５】

図１５

1101 1201 1202 1203

#	宛先アドレス条件	送信元アドレス条件	中継／廃棄フラグ
1	任意	192.168.3.3	中継
2	192.168.1.1	任意	中継
3	任意	任意	廃棄

【図１７】

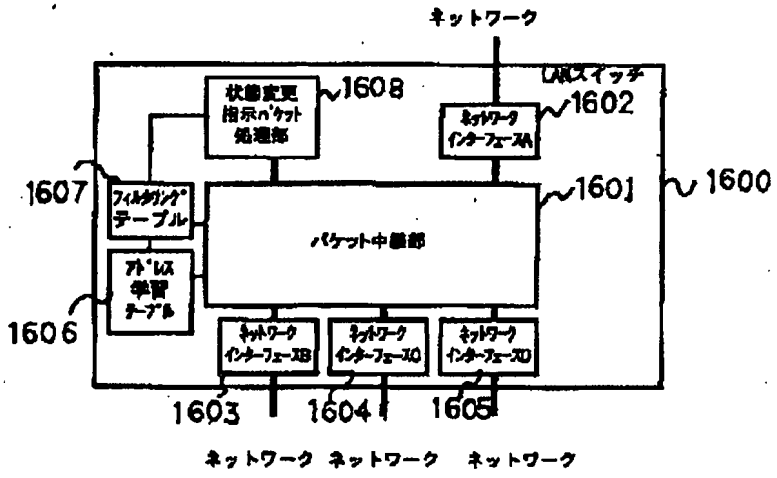
図１７

1607 1701 1702 1703

#	MAC アドレス	IP アドレス	接続ポート
1	22:22:FF:00:00:01	未登録	B

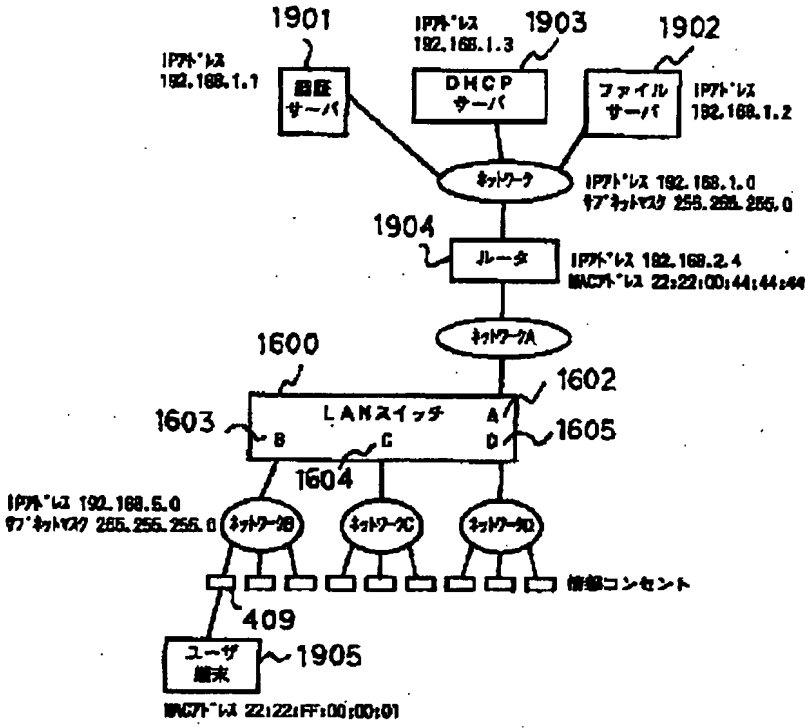
【図１６】

図１６


ネットワーク
状態変更指示パケット処理部
1608
LANスイッチ
ネットワークインターフェースA
1602
1607
フィルタリングテーブル
パケット中継部
1601
1600
アドレス学習テーブル
1606
ネットワークインターフェースB
ネットワークインターフェースC
ネットワークインターフェースD
1603
1604
1605
ネットワーク ネットワーク ネットワーク

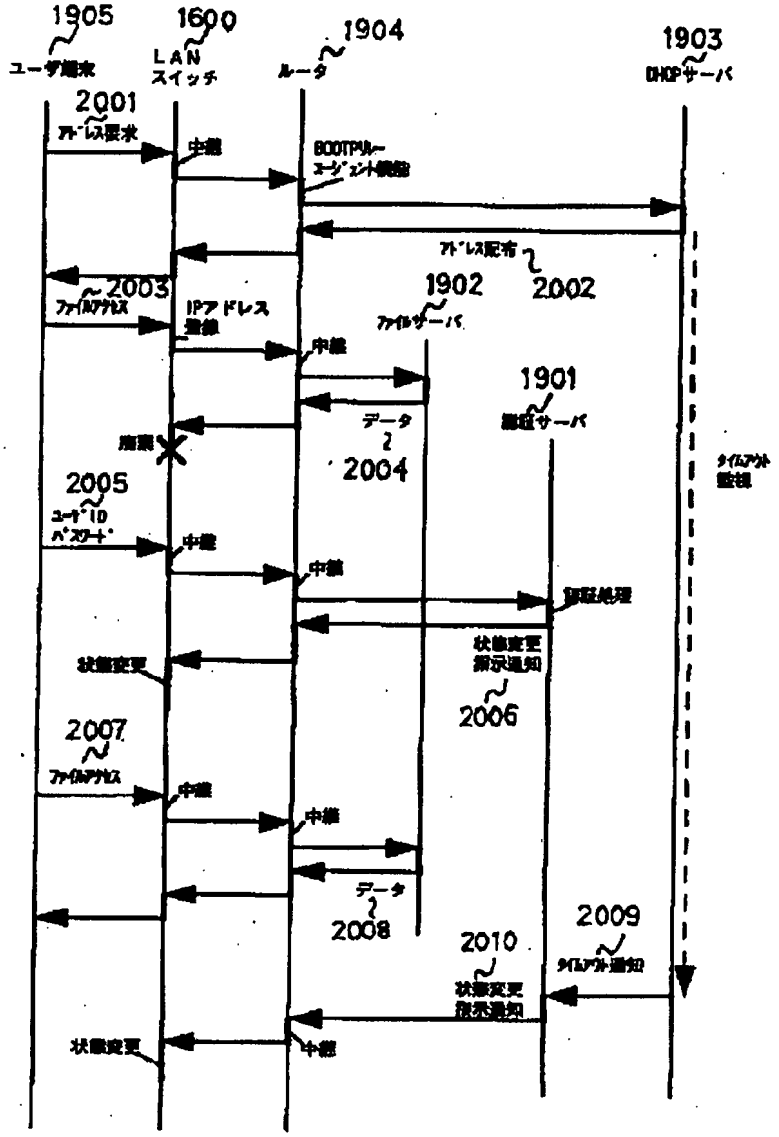
【図１９】

図１９


1901
IPアドレス
192.168.1.1
認証
サーバ
IPアドレス
192.168.1.3
1903
DHCP
サーバ
1902
ファイル
サーバ
IPアドレス
192.168.1.2
ネットワーク
IPアドレス 192.168.1.0
サブネットマスク 255.255.255.0
1904
ルータ
IPアドレス 192.168.2.4
MACアドレス 22:22:00:44:44:44
ネットワークA
1600
1602
LANスイッチ
A
B
C
D
1603
1605
1604
IPアドレス 192.168.5.0
サブネットマスク 255.255.255.0
ネットワークB
ネットワークC
ネットワークD
情報コンセント
409
ユーザ
端末
1905
MACアドレス 22:22:FF:00:00:01

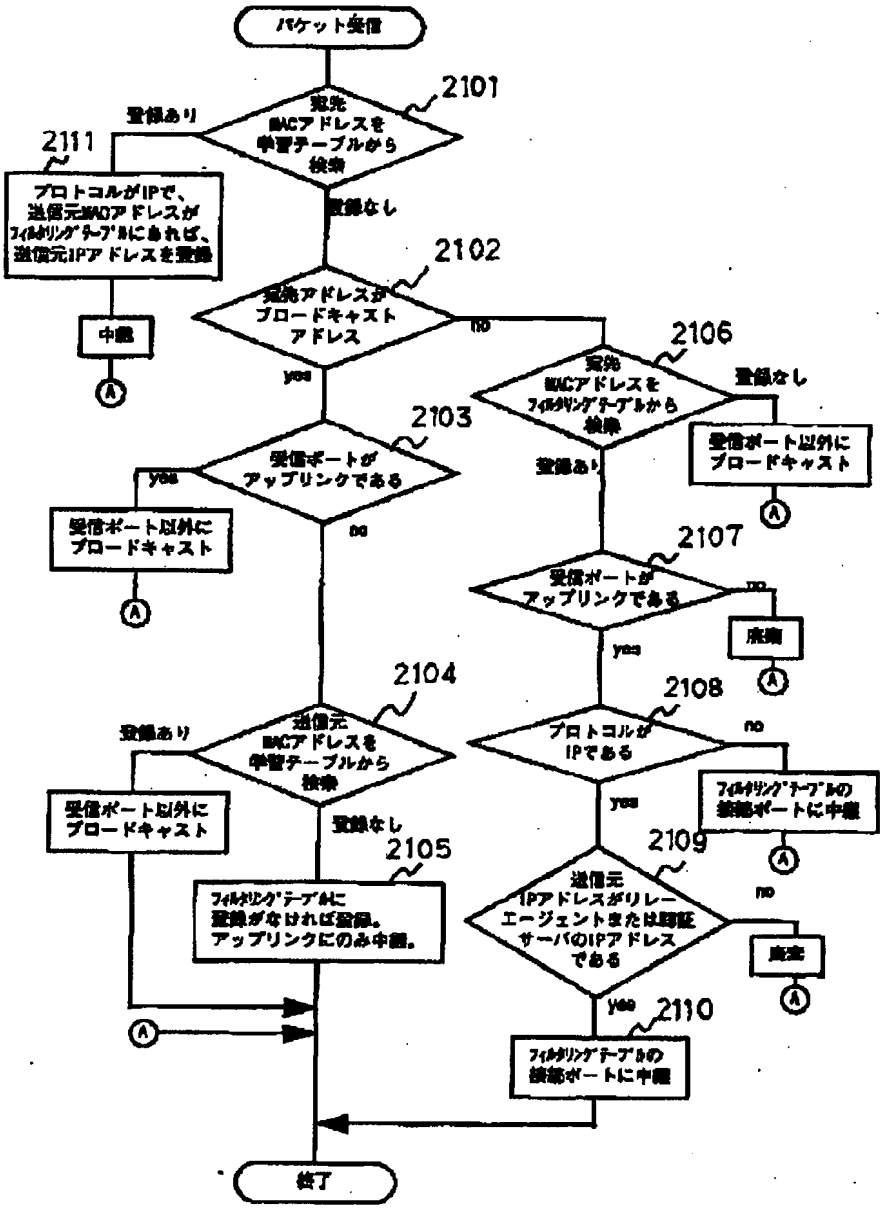
【図２０】

図２０


1905
1600
LAN
スイッチ
1904
ルータ
1903
DHCPサーバ
2001
中継
2002
2003
IPアドレス
中継
1902
1901
データ
2004
2005
中継
中継
状態変更
2006
2007
中継
中継
データ
2008
2009
2010
状態変更
中継

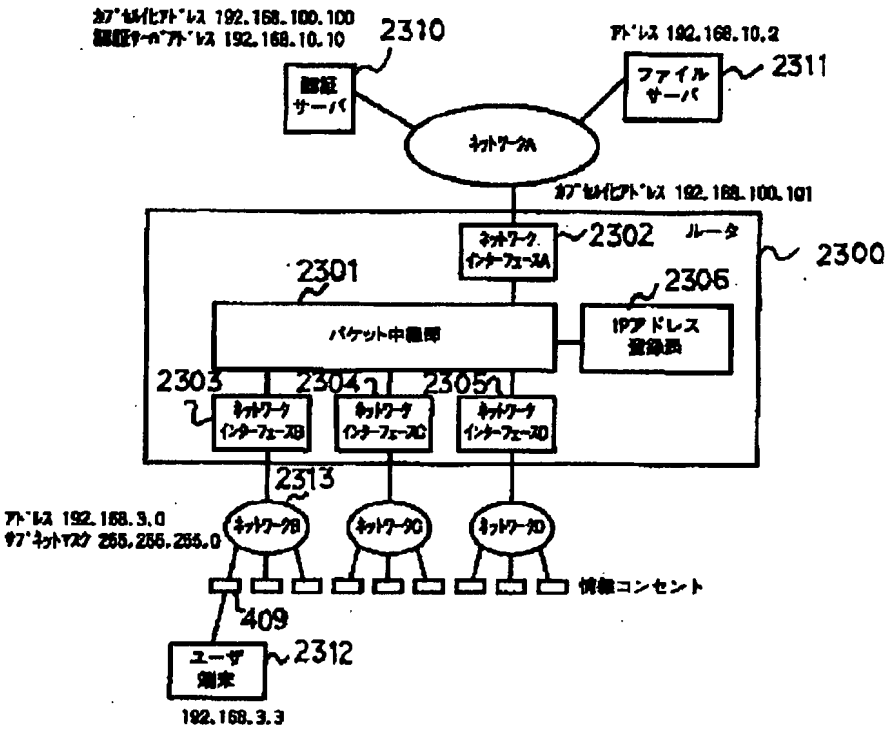
【図２１】

図２１


パケット受信
2101
宛先MACアドレスを学習テーブルから検索
登録あり
登録なし
2111
プロトコルがIPで、送信元MACアドレスがフィルタリングテーブルにあれば、送信元IPアドレスを登録
中継
2102
宛先アドレスがブロードキャストアドレス
yes
no
2103
受信ポートがアップリンクである
yes
no
受信ポート以外にブロードキャスト
2104
送信元MACアドレスを学習テーブルから検索
登録あり
登録なし
受信ポート以外にブロードキャスト
2105
フィルタリングテーブルに登録がなければ登録。アップリンクにのみ中継。
2106
宛先MACアドレスをフィルタリングテーブルから検索
登録なし
登録あり
受信ポート以外にブロードキャスト
2107
受信ポートがアップリンクである
no
yes
廃棄
2108
プロトコルがIPである
no
yes
フィルタリングテーブルの該当ポートに中継
2109
送信元IPアドレスがリレーエージェントまたは認証サーバのIPアドレスである
no
yes
廃棄
2110
フィルタリングテーブルの該当ポートに中継
終了

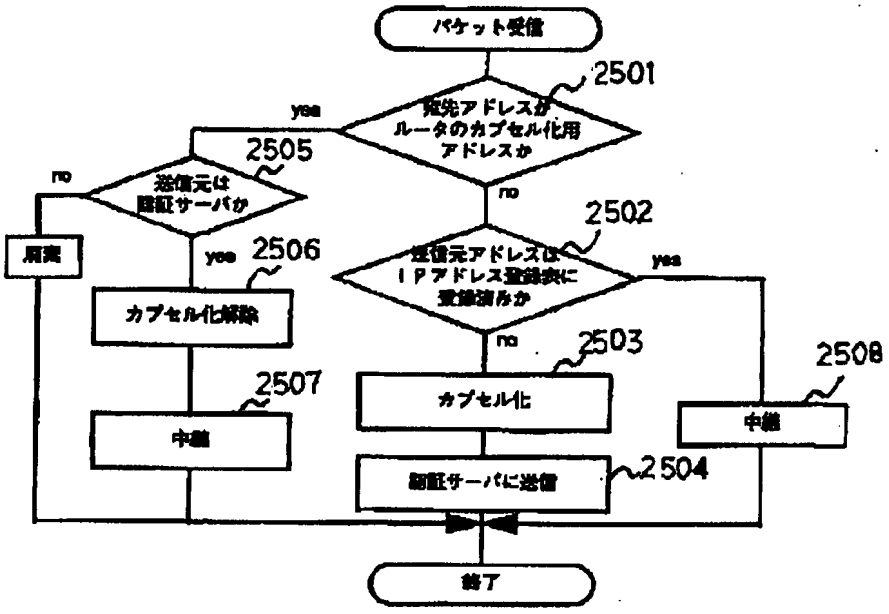
【図２３】

図２３


2310
2311
2302
ルータ
2300
2301
2306
2303
2304
2305
2313
409
2312
192.168.3.3

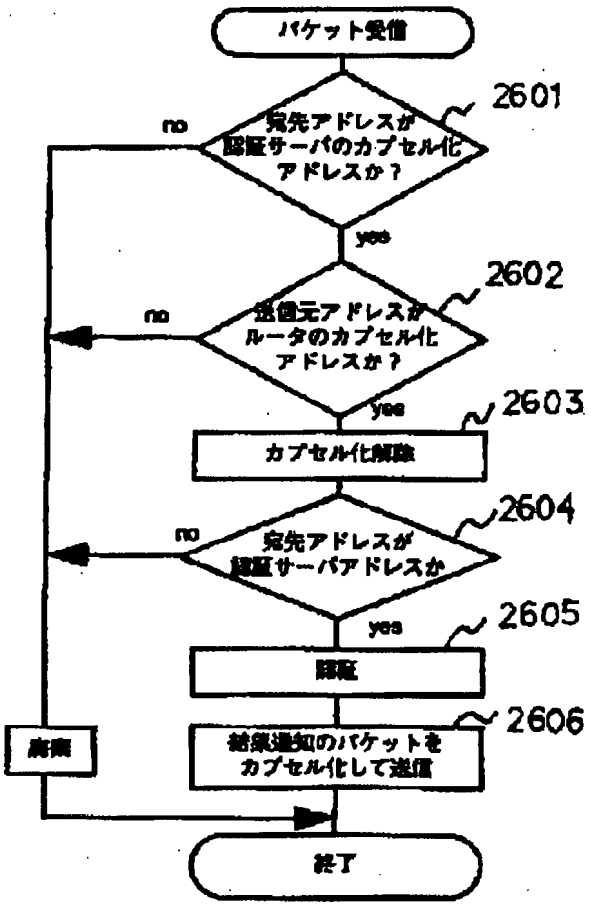
【図２５】

図２５


パケット受信
2501
宛先アドレスが
ルータのカプセル化用
アドレスか
yes
no
2505
送信元は
認証サーバか
no
yes
2502
送信元アドレスは
IPアドレス登録表に
登録済みか
yes
no
2506
カプセル化解除
2503
カプセル化
2508
中継
2507
中継
認証サーバに送信
2504
終了

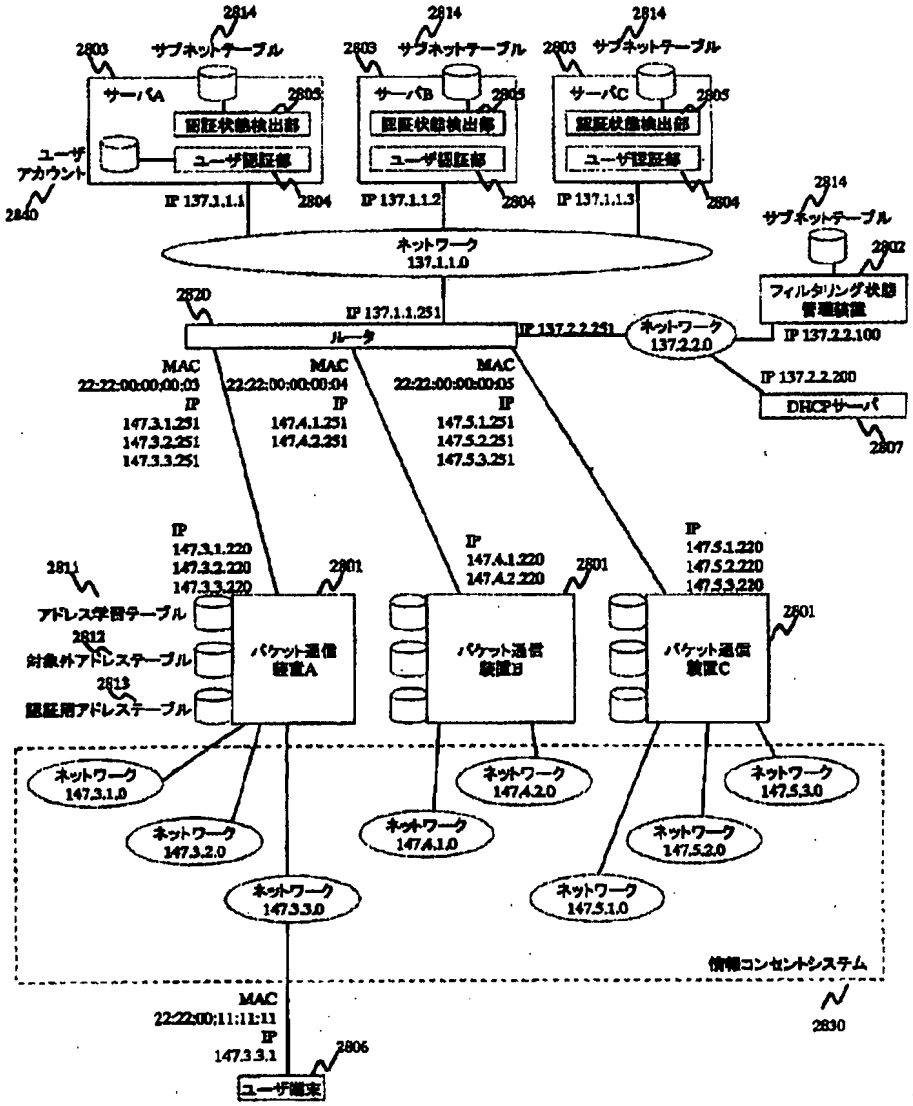
【図２６】

図２６


パケット受信
2601
宛先アドレスが
認証サーバのカプセル化
アドレスか？
no
yes
2602
送信元アドレスが
ルータのカプセル化
アドレスか？
no
yes
2603
カプセル化解除
2604
宛先アドレスが
認証サーバアドレスか
no
yes
2605
認証
2606
結果通知のパケットを
カプセル化して送信
廃棄
終了

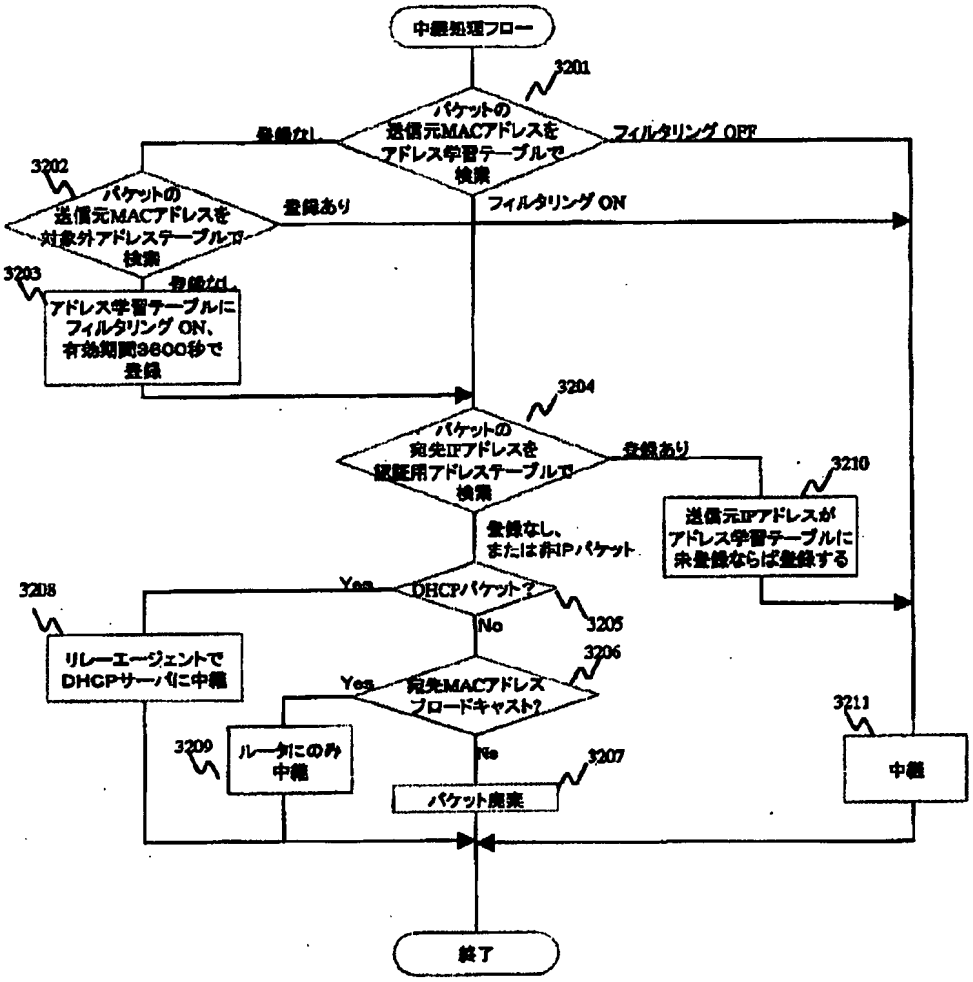
【図２８】

図28


2814
サブネットテーブル
2803
サーバA
2805
認証状態検出部
ユーザ認証部
ユーザアカウント
2840
IP 137.1.1.1
2804
サーバB
IP 137.1.1.2
サーバC
IP 137.1.1.3
ネットワーク
137.1.1.0
2820
ルータ
IP 137.1.1.251
IP 137.2.2.251
ネットワーク
137.2.2.0
2802
フィルタリング状態
管理装置
IP 137.2.2.100
IP 137.2.2.200
DHCPサーバ
2807
MAC
22:22:00:00:00:03
IP
147.3.1.251
147.3.2.251
147.3.3.251
22:22:00:00:00:04
147.A.1.251
147.A.2.251
22:22:00:00:00:05
147.5.1.251
147.5.2.251
147.5.3.251
IP
147.3.1.220
147.3.2.220
147.3.3.220
2811
アドレス学習テーブル
2812
対象外アドレステーブル
2813
認証用アドレステーブル
2801
パケット通信
装置A
147.A.1.220
147.A.2.220
パケット通信
装置B
147.5.1.220
147.5.2.220
147.5.3.220
パケット通信
装置C
2501
ネットワーク
147.3.1.0
ネットワーク
147.3.2.0
ネットワーク
147.3.3.0
ネットワーク
147.A.2.0
ネットワーク
147.A.1.0
ネットワーク
147.5.3.0
ネットワーク
147.5.2.0
ネットワーク
147.5.1.0
情報コンセントシステム
2830
MAC
22:22:00:11:11:11
IP
147.3.3.1
2806
ユーザ端末

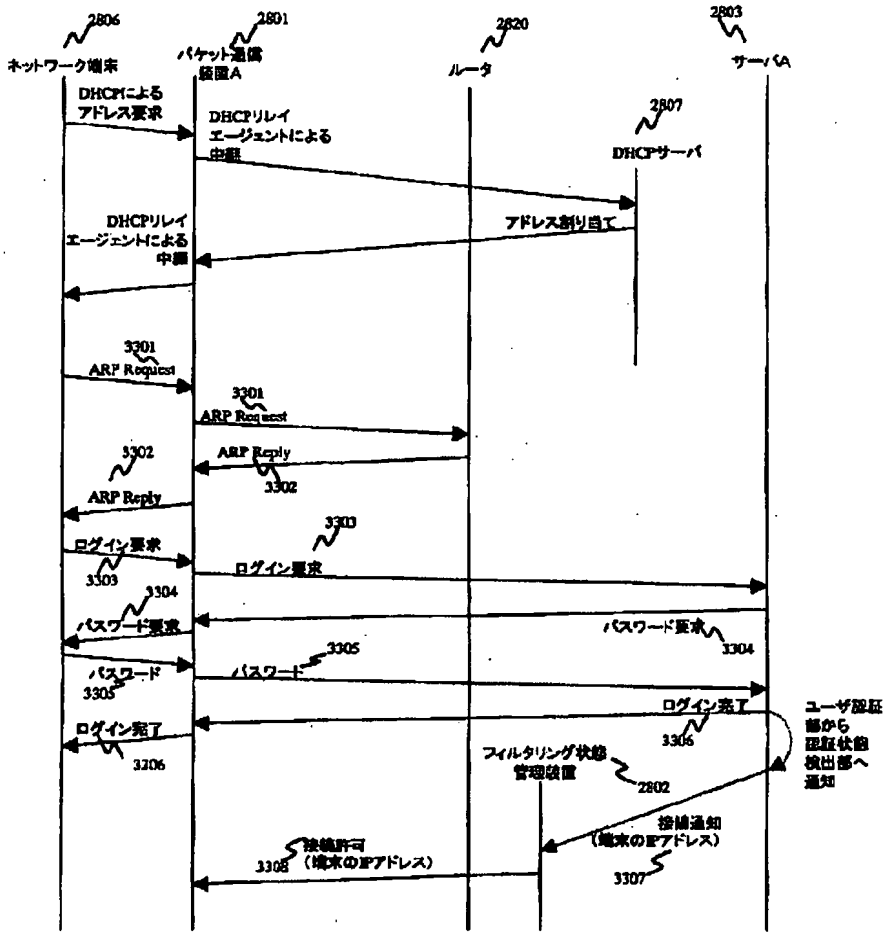
【図３２】

図32


中継処理フロー
3201
パケットの送信元MACアドレスをアドレス学習テーブルで検索
登録なし
フィルタリング OFF
3202
パケットの送信元MACアドレスを対象外アドレステーブルで検索
登録あり
フィルタリング ON
3203
登録なし
アドレス学習テーブルにフィルタリング ON、有効期間3600秒で登録
3204
パケットの宛先IPアドレスを認証用アドレステーブルで検索
登録あり
3210
送信元IPアドレスがアドレス学習テーブルに未登録ならば登録する
登録なし、またはIPパケット
Yes
DHCPパケット?
No
3205
3208
リレーエージェントでDHCPサーバに中継
3206
Yes
宛先MACアドレスブロードキャスト?
3211
3209
ルータにのみ中継
No
3207
パケット廃棄
中継
終了

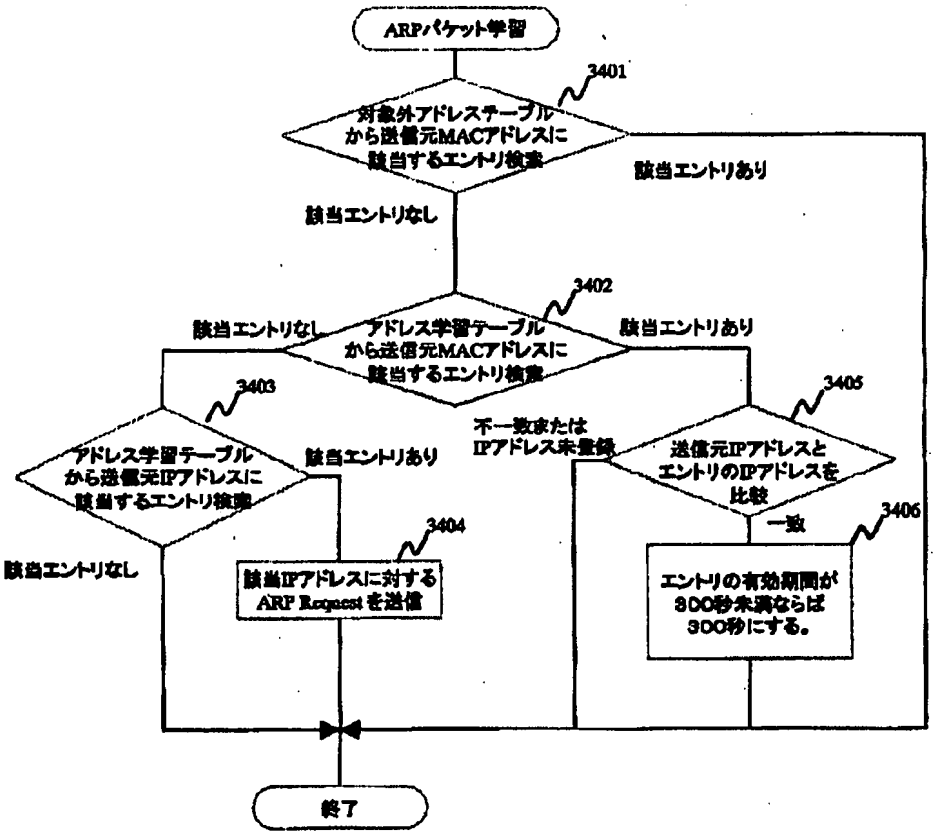
【図３３】

図33


2806
ネットワーク端末
2801
パケット通信
装置A
2820
ルータ
2803
サーバA
2807
DHCPサーバ
DHCPによる
アドレス要求
DHCPリレイ
エージェントによる
中継
アドレス割り当て
DHCPリレイ
エージェントによる
中継
3301
ARP Request
3301
ARP Request
ARP Reply
3302
3302
ARP Reply
3303
ログイン要求
3303
ログイン要求
3304
パスワード要求
パスワード要求
3304
3305
パスワード
3305
パスワード
ログイン完了
3306
ユーザ認証
部から
認証状態
検出部へ
通知
ログイン完了
3306
フィルタリング状態
管理装置
2802
接続通知
（端末のIPアドレス）
3307
接続許可
3308
（端末のIPアドレス）

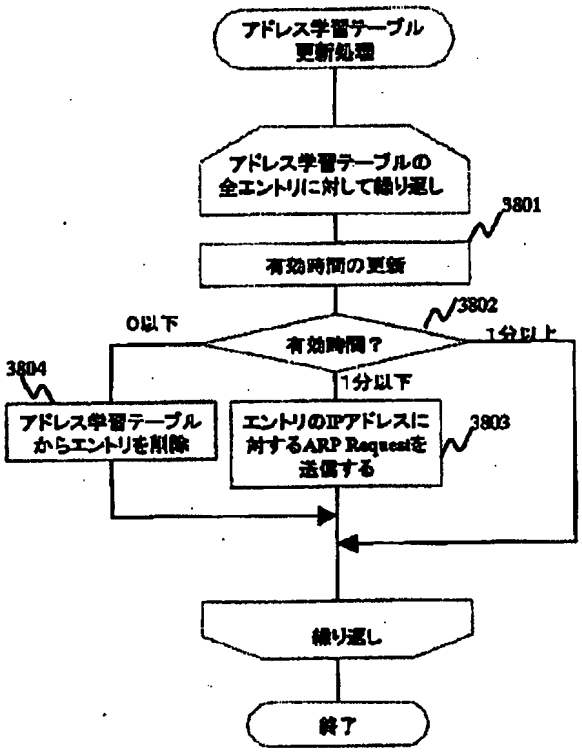
【図３４】

図34


ARPパケット学習
3401
対象外アドレステーブル
から送信元MACアドレスに
該当するエントリ検索
該当エントリあり
該当エントリなし
3402
該当エントリなし
アドレス学習テーブル
から送信元MACアドレスに
該当するエントリ検索
該当エントリあり
3403
3405
不一致または
IPアドレス未登録
アドレス学習テーブル
から送信元IPアドレスに
該当するエントリ検索
該当エントリあり
送信元IPアドレスと
エントリのIPアドレスを
比較
3404
一致
3406
該当エントリなし
該当IPアドレスに対する
ARP Request を送信
エントリの有効期間が
300秒未満ならば
300秒にする。
終了

【図３８】

図38



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04L 12/56		H04L 12/56	B
	100		100Z

(72)発明者 野崎 信司
神奈川県秦野市堀山下１番地 株式会社日立製作所エンタープライズサーバ事業部内
(72)発明者 巽 義行
東京都江東区新砂一丁目６番27号 株式会社日立製作所公共システム事業部内

Fターム(参考) 5K030 GA15 HA08 HB18 HC14 HD03 HD07 HD10 KA05 KA13 KX24 LB05 LC13 LD20
5K033 AA08 CB01 CB08 CC01 DA01 DA05 DB12 DB19 EA07 EC01 EC04